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

DONNA CURLING, ET AL., Plaintiffs, v. BRIAN KEMP, ET AL., Defendants.	Civil Action No. 1:17-CV-2989-AT

DECLARATION OF J. ALEX HALDERMAN
IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

J. ALEX HALDERMAN declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1.   My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Declaration in support of Plaintiffs Donna Curling, Donna Price, and Jeffrey Schoenberg (the "Curling Plaintiffs").

2.   I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

3.   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.

4.   I have authored more than 80 articles and books. My work has been cited in more than 6,900 scholarly publications. I have served on the program committees for 30 research conferences and workshops, and I co-chaired the USENIX Electronic Voting Technology Workshop, which focuses on electronic voting security. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938 E Award for teaching and scholarship.

5.   I have published peer-reviewed research analyzing the security of electronic voting systems used in numerous U.S. states as well as in other countries. I have also investigated methods for improving the security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records. I have testified before the U.S. Senate Select Committee on Intelligence on the subject of cybersecurity and U.S. elections.

6.   I have performed extensive hands-on security testing of the AccuVote

TS and TSX electronic voting machines, which I understand are the two models of

electronic voting machines used in Georgia. I published a peer-reviewed security

evaluation of the AccuVote TS[1], and I performed a source code review of the

AccuVote TSX as part of a study commissioned by the Secretary of State of

California.[2] These studies discovered dozens of serious security vulnerabilities in

the AccuVote hardware and software.

7.   My curriculum vitae, including a list of honors and awards, research

projects, and publications, is attached as Exhibit A.

Context: Cyberattacks, the 2016 Presidential Election, and Upcoming Elections

8.   The 2016 presidential election was subject to unprecedented

cyberattacks apparently intended to interfere with the election and undermine

confidence in the voting process. For example, attackers broke into the email

system of the Democratic National Committee and, separately, into the email

account of John Podesta, the chairman of Secretary Clinton's campaign. Exhibits

---

[1] 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.
[2] Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System*, University of California, Berkeley (2007), http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.

B and C. The attackers leaked private messages from both hacks. Attackers also

attempted to breach election-related systems in at least 18 states, including

Georgia. Exhibit D.[3] In at least two states, Illinois and Arizona, these attackers

successfully infiltrated the voter registration systems and stole voter data. Exhibit

E. The U.S. Senate Select Committee on Intelligence has concluded that, in a

small number of states, the attackers were in a position to alter or delete voter

registration data.[4] Exhibit F. The Department of Homeland Security has stated

that senior officials in the Russian government commissioned these attacks.

Exhibit G.

9.   Russia has sophisticated cyber-offensive capabilities, and it has shown

a willingness to use them to hack elections elsewhere. 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 could

---

[3] Kim Zetter, *Was Georgia's Election System Hacked in 2016?*, POLITICO
Magazine (July 18, 2018),
https://www.politico.com/magazine/story/2018/07/18/mueller-indictments-
georgia-voting-infrastructure-219018.
[4] Senate Intelligence Committee, *Russian Targeting of Election Infrastructure
During the 2016 Election: Summary of Initial Findings and Recommendations*, at
1-2 (May 9, 2018), https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-
%20ElecSec%20Findings,Recs2.pdf.

have caused the wrong winner to be announced. Exhibit H. Countries other than Russia also have similarly sophisticated cyberwarfare capabilities.

10.   In May 2018, the U.S. Senate Select Committee on Intelligence, charged with investigating cybersecurity threats to U.S. election infrastructure, reported its findings and recommendations.[5] The committee found serious vulnerabilities, including that "voting systems across the United States are outdated, and many do not have a paper record of votes as a backup counting system that can be reliably audited, should there be allegations of machine manipulation."[6] Moreover, "Paperless Direct Recording Electronic (DRE) voting machines"—the type used in Georgia—"are at highest risk for security flaws."[7]

11.   Director of National Intelligence Dan Coats and Secretary of Homeland Security Kristjen Nielsen have warned as recently as August 2, 2018, that Russia is continuing to pursue its goal of interfering in our elections, including the upcoming midterm elections in November.[8]

12.   Foreign governments could attempt to hack American voting machines to achieve a variety of goals, including undermining voter confidence

---

[5] Id.

[6] Id. at 4.

[7] Id.

[8] Brian Ries & Meg Wagner, White House press briefing, CNN (Aug. 2, 2018), https://www.cnn.com/politics/live-news/whpb-08-02-18/h_b4373e9f04f5da63237586ce450a0962.

and causing fraudulent outcomes. They could sabotage the machines to prevent

them from functioning on Election Day, or to cause them to produce obviously

incorrect results when votes are counted. They could also infiltrate the machines

with malicious software in order to cause them to produce plausible but fraudulent

results. I have written demonstration malicious software that executes these

attacks against the models of electronic voting machines used in Georgia.

The Vulnerability of Georgia's Voting Machines to Cyberattack

13.   More than 70% of American voters have their votes recorded on some

form of paper, which provides permanent evidence of their intent in the event of a

post-election audit or recount—33 states have a paper ballot, or at least a paper

trail, for every vote. In Georgia, except for absentee voting, all ballots are cast on

paperless[9] direct-recording electronic (DRE) computer voting machines that do not

create a paper record of each vote. Georgia is one of only five states to use

paperless machines statewide.[10]

_____

[9] In election technology contexts, "paperless" refers to machines that lack a voter-verifiable paper record of each ballot. Although Georgia's machines print a paper summary of the election totals after polls close, they are still considered "paperless," since this summary tape does not provide a way for the voter to confirm that his or her vote has been properly recorded.
[10] Verified Voting, The Verifier – Polling Place Equipment – November 2018, https://www.verifiedvoting.org/verifier/ (last accessed Aug. 7, 2018).

14.   Paperless DRE voting machines have been repeatedly shown to be vulnerable to cyberattacks that can change or erase votes, cast extra votes, or cause the machines to fail to operate on election day. Since paperless DREs do not generate a physical record of the vote, these attacks may be difficult or impossible to detect or to reverse. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.

15.   To my knowledge, Georgia exclusively uses Premier/Diebold (Dominion) AccuVote TS and TSX voting machines. These particular models are probably the most well-studied by security researchers of any voting machines in the world. Over the past 15 years, I and other experts have repeatedly documented serious cybersecurity problems with these machines, in peer-reviewed and state-sponsored research studies. The vulnerabilities that affect Georgia's machines include numerous hardware and software security flaws, as well as architectural weaknesses that cannot be repaired through software updates. As a result, every DRE in use in Georgia is vulnerable to cyberattacks.

16.   These voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. In tests, I have demonstrated that, in just a few seconds, anyone can install vote-stealing

malware on these voting machines that will silently alter all records of every vote.[11]

17.   The first major study of these machines was carried out in 2003 by Kohno, Stubblefield, Rubin, and Wallach, who studied a leaked version of the source code and found many design errors and vulnerabilities.[12] Public concern in light of Kohno's study led the state of Maryland to authorize two security studies. The first, by SAIC, reported that the system was "at high risk of compromise."[13] The second, conducted by RABA, a security consulting firm, confirmed many of Kohno's findings and suggested design changes to the Diebold system.[14] A further security assessment was commissioned by the Ohio Secretary of State and carried

---

[11] A video documenting this result is publicly available. Hack247, *Princeton University Diebold Machine Hacking*, YouTube (Nov. 7, 2006), https://www.youtube.com/watch?v=2Vvq_YseZVc.

[12] Tadayoshi Kohno et al., *Analysis of an Electronic Voting System*, *in* IEEE Symposium on Security and Privacy, IEEE Computer Society Press (Feb. 27, 2004), http://avirubin.com/vote.pdf.

[13] Science Applications International Corporation, Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes, SAIC-6099-2003-261 (Sept. 2, 2003).

[14] RABA Technologies, *Trusted agent report: Diebold AccuVote-TS voting system*, (Jan. 20, 2004), http://euro.ecom.cmu.edu/program/courses/tcr17-803/TA_Report_AccuVote.pdf.

out by Compuware.[15] It examined several DRE systems, including the AccuVote

TS, and identified a number of high-risk security problems.

18.   In 2006, independent security researcher Harri Hursti examined the

hardware and firmware of AccuVote TS and TSX systems. He discovered

problems with a software update mechanism that could allow malicious parties to

infect the machines with malicious code.[16] Also in 2006, I and collaborators at

Princeton obtained an AccuVote TS from a private party and reverse engineered its

hardware and software.[17] Our study confirmed the results of the earlier security

reviews and discovered a variety of additional serious vulnerabilities.

19.   We demonstrated the vulnerabilities of the AccuVote TS by

developing a piece of malware (malicious software) that could infect the machines

and steal votes. The malware modifies all of 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

_____

[15] Compuware Corp., *Direct recording electronic (DRE) Technical Security Assessment Report* (Nov. 21, 2003), http://www.sos.state.oh.us/sos/hava/compuware112103.pdf.
[16] Harri Hursti, *Diebold TSx Evaluation Security Alert: May 11, 2006 Critical Security Issues with Diebold TSx*, IssueLab (May 11, 2006), https://www.issuelab.org/resources/1294/1294.pdf.
[17] Feldman, *supra* note 1.

necessary to ensure that the attacker's favored candidate always had at least a certain percentage of the vote total.

20.   We also developed a voting machine virus that could spread the vote-stealing malware automatically and silently from machine to machine during normal pre- and post-election activities. The virus propagated via the removable memory cards that election officials 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.

21.   Once installed, the virus copies itself to every memory card inserted into the infected machine. If those cards were inserted into other machines, they too would become infected. As a result, an attacker could infect a large population of machines while only having temporary physical access to a single machine or memory card.

22.   In 2007, the Secretary of State of California organized a comprehensive election security examination, the California Top-to-Bottom Review (TTBR[18]), which examined systems including the AccuVote TSX. I was part of a team of six experts who spent approximately 30 days examining the

_____

[18] Cal. Sec'y of State, *Top-to-Bottom Review*, http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ (last accessed Aug. 7, 2018).

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[19]),

which also covered the AccuVote TSX system.

23.   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.

24.   Some of the software vulnerabilities that affect the AccuVote

machines can be corrected by improving the AccuVote software. For example,

more recent versions of the AccuVote software have been modified to properly

authenticate software updates, closing one of several routes by which malware

could infect the machines. However, other vulnerabilities reflect deeper

architectural problems that cannot be corrected through software changes. Since all

---

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

records of the vote are under software control, if there is any way for malware to infect the machine, the election results can be compromised.

25.   The software that performs election functions on the AccuVote TS and TSX is called BallotStation. I understand that the machines used in Georgia use BallotStation version 4.5.2!, which I understand was developed in 2005. This software predates the California and Ohio studies, which examined version 4.6 in 2007. Therefore, it is almost certain that the serious vulnerabilities discovered in these studies remain uncorrected in the software on Georgia's machines.

26.   I myself have developed demonstration vote-stealing malware that exploits vulnerabilities in BallotStation 4.3, 4.4, and 4.6—versions that closely predate and follow the software version used in Georgia.[20] Based on my examination of changes in the software that occurred between versions 4.4 and 4.6, I believe that similarly serious vulnerabilities are all but certain to affect Georgia's machines.

27.   Moreover, the AccuVote TS and TSX machines rely on Windows CE as their operating system. This software has not been supported by Microsoft in

_____

[20] I recently demonstrated for the New York Times an attack that can remotely steal votes on the AccuVote TSX. The demonstration machine used BallotStation 4.6. *See* Matteen Mokalla, Taige Jensen & J. Alex Halderman, I Hacked an Election. So Can the Russians., N.Y. Times (Apr. 5, 2018), https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russ%20ians.html.

several years[21] and has been shown to have significant vulnerabilities itself, beyond

those of the election-specific software.[22] Georgia's machines apparently have not

had this operating system software updated since at least 2005.

28.   Based on the results of the TTBR, California decertified the Accuvote

TSX in 2007.[23] This was the case even though California's machines, unlike

Georgia's, produced a voter-verifiable paper trail that could be used to detect and

correct vote-stealing attacks. Georgia's machines have no such protection and

apparently have not received software updates to correct any of the many security

flaws discovered over the last 13 years, yet they remain in use.

Vulnerabilities in Georgia's Machines Could Be Used to Attack Elections on a Wide Scale

29.   The security features built into Georgia's voting machines are

inadequate to defend against cyberattacks. Whether voting machines are

connected to the Internet is irrelevant. Sophisticated attackers, such as nation-

states, have developed a variety of techniques for attacking non-Internet-connected

---

[21] Microsoft, Inc., *Search product lifecycle*, https://support.microsoft.com/en-us/lifecycle/search (search "Microsoft Windows CE .NET 4.0").
[22] CVE Details, Microsoft > Windows Ce: Vulnerability Statistics, https://www.cvedetails.com/product/1079/Microsoft-Windows-Ce.html?vendor_id=26 (last accessed Aug. 7, 2018).
[23] Cal. Sec'y of State, *Withdrawal of Approval of Diebold Election Systems, Inc.* (revised Oct. 25, 2007), http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf.

systems.[24] There are several routes by which such attackers might infect Georgia's machines with malicious software.

30. Shortly before each election, poll workers must program every voting machine in Georgia with the ballot design, including the names of the races and candidates. This ballot programming is copied to each machine on a removable memory card, similar to the memory card used in a digital camera. If an attacker can modify the ballot programming files, the attacker can piggyback on the pre-election programming process to spread malicious software to the machines.

31. Ballot programming files are typically created by election officials on a regular desktop computer in a government office, or by an election service vendor that creates programming for voting machines across many jurisdictions. The computer software that generates the ballot programming files is called an election management system (EMS). If attackers can access the EMS, they can tamper with the ballot programming files it generates, and thereby spread a vote-stealing attack to voting machines across all jurisdictions serviced by the EMS.

---

[24] 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/.

32.   Moreover, I understand that the primary vendor of Georgia's voting machines has recently announced it installed remote access software on EMS's it sold during the time period in which Georgia purchased its election machines.[25] Any remote access to the software installed on Georgia's election management systems creates a wide open door for hackers.

33.   Furthermore, a local attacker with physical access to the machines can additionally tamper with them by manipulating the machines' removable memory cards. Access to these cards is protected using a low security lock that can be picked using only a paperclip or BIC pen.[26] The machines would have to be perfectly safeguarded at all times, beginning from the time they are manufactured, to avoid the possibility of being infected with malware that would stealthily affect future elections.

34.   Here is one example of how an attack could proceed. Suppose a foreign government were to attempt to hack Georgia's voting machines to influence the outcome of an election. First, the attackers would probe state offices

---

[25] Kim Zetter, Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States, Motherboard (July 17, 2018https://motherboard.vice.com/amp/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states?__twitter_impression=true.

[26] Shown in this video demonstration: Matt Bernhard, Breaking into a voting machine using a pen, YouTube (Oct. 25, 2016), https://www.youtube.com/watch?v=vqNJL0fYwSk.

(or the offices of election service vendors) well in advance to find ways to break into the election management computers. Next, when it was clear which systems were most vulnerable and which races were the closest, the attackers would hijack the pre-election programming process to spread malware into voting machines in parts or all of the state. This malware would be designed to manipulate the machines to shift a few percent of the vote to favor the attacker's desired candidate. One would expect a skilled attacker's work to leave no visible signs.

Procedural Safeguards Are Inadequate to Protect Georgia's Elections

35. Procedural safeguards used by Georgia to protect its voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack.

36. 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 the voting machine. Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers. The types of seals typically used for voting equipment can be bypassed without detection using

readily available tools.[27] For some seals, these include screwdrivers and hair dryers. By bypassing the seals, an attacker with physical access to the voting machines can modify their internal programming to make them output fraudulent results.

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

38.   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 a voting machine can be programmed to detect and circumvent L&A testing. For example, L&A testing on the AccuVote TS and TSX voting machines is typically performed by putting the machines into a special "test mode" that is not used during regular voting. Malware can detect that the machine is in test mode and suppress cheating until actual voting begins. Similarly, both models of voting machine have digital clocks. Malware can be programmed to cheat only

---

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

at the moment polls close on Election Day, so that testing performed at an earlier or later time would show nothing amiss. I myself have programmed malware for the AccuVote TS and TSX voting machines that uses methods similar to these to avoid detection during L&A testing.

39.   I understand that Georgia also employs a testing technique known as "parallel testing." Officials select a small number of voting machines that have been prepared for use in the election and set them aside for testing. Over the course of Election Day, workers cast votes with known selections on these machines. At the end of the day, they compare the results produced by the machines to the known-correct totals.

40.   Parallel testing provides limited and insufficient protection against attacks. Like L&A testing, it can be defeated if malware can detect that testing is taking place. Workers who are casting scripted votes are likely to behave differently from real voters, such as by taking less time to read instructions, and malware could be programmed to detect such differences.

41.   In any event, parallel testing that occurs during or after the election is necessarily too late to prevent attackers from sabotaging the election. If the testing reveals, at the close of the election, that the machines were counting incorrectly,

there will likely be no way to recover the true results, since the machines used in

Georgia have no paper backup records.

42.   However it is practiced, the most that parallel testing can establish is

that the specific machines that were tested counted correctly during the test. If

only a fraction of machines are programmed to cheat—or if all the machines are

programmed to cheat only a fraction of the times they are powered on—parallel

testing would have a low probability of detecting the fraud. Such fraud could

affect a sufficient number of votes to change the outcome of a close race.

43.   Another proposed method of detecting fraud is to look for statistical

anomalies or outliers in the election results and to re-examine the machines or

election data in those localities. This approach is inadequate for several reasons.

44.   First, it is difficult or impossible to *rule out* electronic fraud by re-

examining the machines. At best, it is possible that careful digital forensics would

reveal evidence of fraud if it indeed occurred. However, it is also possible that a

carefully constructed attack would leave no forensic traces, or that what traces

there were would be missed by a cursory re-examination.

45.   For example, if the machines were infected by malware during voting,

such malware could alter all records of the votes then erase itself when polls close.

In this case, nothing would appear to be amiss even if officials re-tallied all the

election data from the machine. I myself have written malware that behaves this way on the AccuVote TS.

46.   Second, even if a careful forensic examination proved that fraud occurred, it would likely be impossible to determine the true vote totals. Suppose that an investigation showed that certain machines were infected with malware that flipped a random percentage of votes from one candidate to another as they were being recorded. Since Georgia's machines have no paper record of individual ballots, the voters' choices would be permanently lost.

47.   Third, a stealthily executed attack would not create tell-tale anomalies or draw attention to specific locations or machines. For instance, an attack that shifted a small fraction of the vote uniformly across an entire house district would be difficult to distinguish from bias in pre-election polling.

48.   Finally, as with parallel testing, investigation after the election is no help if the attacker's intention is to sabotage the voting process. Disruptive attacks—such as preventing machines from turning on in jurisdictions that favor a particular candidate—could cause a partisan shift in the election outcome.

Adopting Paper Ballots and Post-Election Audits Is the Only Practical Way to Safeguard Elections in Georgia

49.   In light of the threat of cyberattacks intended to affect the outcome of the upcoming election; the profound vulnerability of Georgia's voting machines to cyberattack; and the fact that a skilled attacker would leave no outwardly visible evidence of an attack, the only way to reliably safeguard Georgia's voting system against future cyberattacks is to generate and examine physical evidence of voter intent, in the form of a voter-verifiable paper trail. Such a paper trail is not available today in Georgia—except for absentee ballots—given Georgia's 100% electronic system. Only five states, including Georgia, continue to rely exclusively on such paperless machines.

50.   Optical-scan paper ballots are the most widely used voting method in the United States, and they are the most secure technology available for casting votes. In this style of voting system, the voter fills out a paper ballot that is scanned and counted by a computer and retained in a ballot box. (Voters with accessibility needs complete their ballots using assistive technology, such as a ballot marking device provided at the polling place.) This process results in two independent records of each vote: a digital record created by the scanner, and a physical record in the form of the paper ballot.

21

51.   By combining physical and electronic records of each vote, optical-scan paper ballots can achieve a level of security that is much greater than that of electronic voting or traditional hand-counting. The paper ballots provide an individual, physical record of the voter's selections that cannot be changed by malware or other forms of cyberattack, even if the computer scanners used to read the ballots are compromised. At the same time, the digital records provide a safeguard against low-tech attacks, such as physically stuffing the ballot box.

52.   In a post-election audit, officials can use random sampling to efficiently confirm that the paper and digital records reflect the same election outcome. Although a high-tech attacker might still manipulate the digital records, and a group of low-tech criminals with sufficient physical access might manipulate some of the paper records, altering *both* sets of records in a way that reflected the same election outcome would require a truly extraordinary conspiracy.

53.   The paper ballots already used in Georgia (for absentee voters) and other states can be audited or counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether

the voter intended to make a mark. Georgia's optically scanned absentee ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted and audited efficiently.

54.   In March, Congress provided $380 million in new funding to the States under the Help America Vote Act, including more than $10 million to Georgia. The appropriation included a joint explanatory statement of Congress's intent: "states may use this funding to: replace voting equipment that only records a voter's intent electronically with equipment that utilizes a voter-verified paper record; implement a post-election audit system that provides a high-level of confidence in the accuracy of the final vote tally. . . ."[28]

55.   Furthermore, in May, the U.S. Senate Select Committee on Intelligence recommended that "States should rapidly replace outdated and vulnerable voting systems. At a minimum, any machine purchased going forward should have a voter-verified paper trail." In addition, "States should consider implementing more widespread, statistically sound audits of election results."
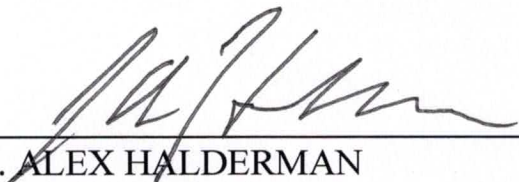
56.   Many states have implemented or are implementing these protections.

---

[28] U.S. Election Assistance Comm'n, HAVA Funds Background (Mar. 30, 2018), https://www.eac.gov/assets/1/6/2018_HAVA_Funds_background.pdf.

Georgia Should Replace DREs With Paper Ballots and Appropriate Post-Election Audits

57.   All of Georgia's votes (that are not cast via absentee ballot) are recorded on DRE voting machines that do not generate any paper record of the individual votes. The only practical way to safeguard Georgia's upcoming election is to discontinue the use of Georgia's DREs, require the use of optical scan paper ballots throughout Georgia, and mandate auditing of the results to ensure that the optical scanners were not attacked with malware to infect the automated counting of the ballots.

Dated: August 7, 2018
        Ann Arbor, Michigan

_____
                J. ALEX HALDERMAN

EXHIBIT A

J. Alex Halderman

Professor, Computer Science and Engineering
University of Michigan

August 7, 2018

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

J.AlexHalderman.com

Research Overview

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

Selected Projects

'17: Weaknesses in TLS interception middleboxes
'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)

Education

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

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

Honors and Awards

– 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")

2

- 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] 403 **Forbidden: A Global View of Geoblocking**
Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, Will Scott, J. A. Halderman, and Roya Ensafi
To appear in *Proc. 18th ACM Internet Measurement Conference* (IMC), October 2018.

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

[3] **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.

[4] **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.

[5] **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.

[6] **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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

5

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] **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.

[31] **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.

[32] **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.

[33] **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.

[34] **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.

[35] **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.

[36] **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.

[37] **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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] **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.

[46] **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.

[47] **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

[48] **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

[49] **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.

[50] **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

[51] **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), August
2017.

[52] **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.

[53] **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.

[54] **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.

[55] **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.

[56] **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.

[57] **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.

[58] **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.

[59] **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.

[60] **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.

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

[62] **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.

[63] **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.

[64] **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.

[65] **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.

[66] **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

[67] **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.

[68] **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.

[69] **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.)

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

[71] **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.

[72] **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.

[73] **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.

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

[75] **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.

[76] **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.

[77] **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.

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

[79] **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

[80] **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.

[81] **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.)

[82] **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.)

[83] **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

[84] **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.

[85] **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. 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.

13

– **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)

– **The Security Impact of HTTPS Interception.** Invited talk, GOTO Copenhagen, Oct. 2, 2017.

– **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.

– **Cybersecurity and U.S. Elections**
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.

– **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: **"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.

– **Congressional Briefing: Free, Automated, and Open Web Encryption.**
August 8, 2017; hosted by Congressional Cybersecurity Caucus.

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

– Moderator: **Apple & the FBI: Encryption, Security, and Civil Liberties.** Panelists: Nate Cardozo and Barbara McQuade. U-M Dissonance Speaker Series, April 12, 2016.

17

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

Post Docs

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

Doctoral Committees

– Denis Bueno (C.S. Ph.D. expected 2018, Michigan) <<<<< HEAD
– Andrew Springall (C.S. Ph.D. 2018, Michigan; chair) =======
– Kyong Tak Cho (C.S. Ph.D. 2018, Michigan)
– Andrew Springall (C.S. Ph.D. 2018, Michigan; chair)
– Armin Sarabi (E.E. Ph.D. 2018, Michigan) >>>>> cafe174a0ef54b0c9772a62bcca30a9a006dba03
– 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)
– 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

– 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 2017, Fall 2016, Fall 2015, Fall 2014, Fall 2013, Fall 2011, Fall 2010, Fall 2009
Created new undergrad security elective that has grown to reach >750 students/year. An accessible intro, teaches the security mindset and practical skills for building and analyzing security-critical systems.

– **Computer and Network Security**, EECS 588, University of Michigan
Terms: Winter 2016, Winter 2015, Winter 2014, Winter 2013, Winter 2012, Winter 2011, Winter 2010, Winter 2009
Redesigned core grad-level security course. Based around discussing classic and current research papers and performing novel independent work. Provides an intro. to systems research for many students.

– **Securing Digital Democracy**, Coursera (MOOC)
Designed and taught a massive, open online course that explored the security risks—and future potential—of electronic voting and Internet voting technologies; over 20,000 enrolled students.

Professional Service

Program Committees

– 2017 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 for the Internet Security Research Group (2014–present)
– Board of Advisors for the Verified Voting Foundation (2012–present)
– External Advisory Board for the DemTech Project, IT University of Copenhagen (2011–present)
– Advisory Council for the Princeton University Department of Computer Science (2012–2014)

Department and University Service

– Faculty Advisor for Michigan Hackers student group (2012–present)
– CSE Graduate Affairs Committee (member, 2014–2017)
– 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)

EXHIBIT B

APRIL GLASER   SECURITY   07.27.16   9:30 AM

HERE'S WHAT WE KNOW ABOUT RUSSIA AND THE DNC HACK
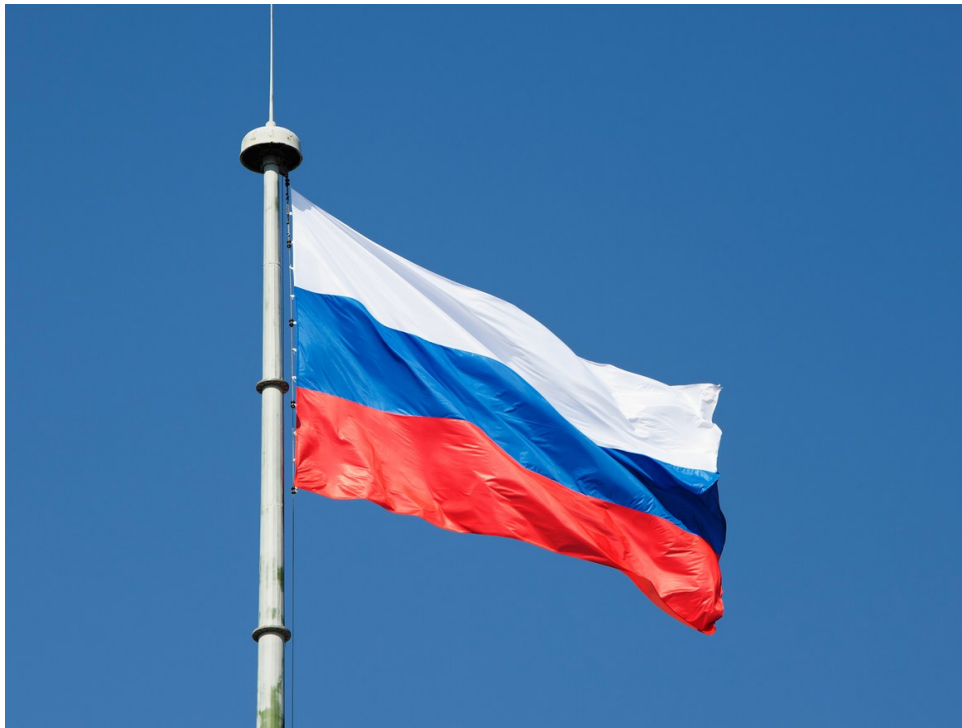
GETTY IMAGES

AS THE DEMOCRATIC National Convention continues its week-long stay in Philadelphia, accusations of Russian hacking continue to cloud the proceedings. At this point, it seems likely that Russia is responsible. What's less clear is what that will mean going forward.

It's been a bad stretch for the Democratic National Committee. Hackers broke into its servers months ago, stealing private emails, opposition research, and campaign correspondence. Last Friday, Wikileaks made nearly 20,000 of those private emails public, revealing embarrassing details of the political machine's inner workings. DNC official allege that the Russian government is behind the breach. The *New York Times* reports that US intelligence agencies increasingly share that opinion. According to a number of top cybersecurity researchers, they're probably right.

A Brief History of a Hack

News of the hack of the Democratic National Committee first broke in mid-June. That's when Crowdstrike, a firm that analyzes threats to network security, revealed that the DNC had called it in to inspect the party's servers, where it found "two separate Russian intelligence-affiliated adversaries present in the DNC network." Crowdstrike released a comprehensive report of its findings on June 14, which accompanied a *Washington Post* article detailing the attacks. One of the hacking groups, Crowdstrike found, had access to the DNC servers for almost a year.

A day after that report, someone calling themselves Guccifer 2.0 (an allusion to notorious hacker Guccifer) claimed responsibility for the hack in a blog post. Through the blog and an accompanying Twitter account, Guccifer 2.0 refuted Crowdstrike's claims that this was a Russian operation, instead calling himself a "lone hacker." He also claimed to have handed much of the DNC bounty to Wikileaks.

The following week, two cybersecurity firms, Fidelis Cybersecurity and Mandiant, independently corroborated Crowdstrike's assessment that Russian hackers infiltrated DNC networks, having found that the two groups that hacked into the DNC used malware and methods identical to those used in other attacks attributed to the same Russian hacking groups.

But some of the most compelling evidence linking the DNC breach to Russia was found at the beginning of July by Thomas Rid, a professor at King's College in London, who discovered an identical command-and-control address hardcoded into the DNC malware that was also found on malware used to hack the German Parliament in 2015. According to German security officials, the malware originated from Russian military intelligence. An identical SSL certificate was also found in both breaches.

The evidence mounts from there. Traces of metadata in the document dump reveal various indications that they were translated into Cyrillic. Furthermore, while Guccifer 2.0 claimed to be from Romania, he was unable to chat with Motherboard journalists in coherent Romanian. Besides which, this sort of hacking wouldn't exactly be outside of Russian norms.

"It doesn't strain credulity to look to the Russians," says Morgan Marquis-Boire, a malware expert with CitizenLab. "This is not the first time that Russian hackers has been behind intrusions in US government, and it seems unlikely that it will be the last." Last year Russian hackers were able to breach White House and State

Department email servers, gleaning information even from President Obama's Blackberry.

Meanwhile, the Kremlin has denied Russian involvement in the DNC breach. But the reverberations continue; DNC Chairwoman Debbie Wasserman Schultz will resign at the end of the week, after emails revealed what many view as the unfair treatment of Bernie Sanders.

From Russia With Love

As compelling as the evidence is, there's still a small amount of room to argue that Guccifer 2.0 was a lone actor, an individual motivated by hacktivist ideals of dismantling state power. He wouldn't be the first. And in a recent interview on NBC, Julian Assange of Wikileaks gave a soft disavowal of claims that his whistleblowing organization is in cahoots with Russian intelligence, "Well, there is no proof of that whatsoever," he said. "We have not disclosed our source, and of course, this is a diversion that's being pushed by the Hillary Clinton campaign."

This is, of course, the same Assange who boasts responsibility for helping find Snowden a home in Russia and Wikileaks publicly criticized the Panama Papers for implicating Putin in financial misdeeds. He's also an outspoken frequent critic of Hillary Clinton's time at the State Department. A damning document dump the weekend before Clinton's nomination arguably aligns with both Russian interests and his own.

If the allegations do prove correct, this is an unprecedented step for Russia. Hacking is nothing new, but publicizing documents to attempt to sway an election certainly is. Putin would clearly prefer a Trump presidency. The billionaire Republican candidate is a longtime admirer of Putin's, and has publicly stated that he wouldn't necessarily defend NATO allies against a Russian invasion. To top it all off, Trump's campaign manager, Paul Manafort, formerly worked as an advisor to Viktor Yanukovych, the Russian-backed President of Ukraine before he was ousted in 2014.

"Due to the nature and timing of this hack, it all seems very political," says Marquis-Boire.

And there's a whole lot of election left—and likely more leaks to come with it. On Sunday, a Twitter user asked Wikileaks if more DNC leaks were on their way. The reply: "We have more coming."

Update: In a press conference Wednesday, Republican presidential candidate Donald Trump invited Russia to retrieve "missing" emails from Hillary Clinton's campaign and release them. Cybersecurity experts described the remarks as "unprecedented" and "possibly illegal."

EXHIBIT C

The New York Times | http://nyti.ms/2eqNSVY

Private Security Group Says Russia Was Behind John Podesta's Email Hack

By **NICOLE PERLROTH** and **MICHAEL D. SHEAR**   OCT. 20, 2016

SAN FRANCISCO — At the start of 2014, President Obama assigned his trusted counselor, John D. Podesta, to lead a review of the digital revolution, its potential and its perils. When Mr. Podesta presented his findings five months later, he called the internet's onslaught of big data "a historic driver of progress." But two short years later, as chairman of Hillary Clinton's presidential campaign, Mr. Podesta would also become one of the internet's most notable victims.

On Thursday, private security researchers said they had concluded that Mr. Podesta was hacked by Russia's foreign intelligence service, the GRU, after it tricked him into clicking on a fake Google login page last March, inadvertently handing over his digital credentials.

For months, the hackers mined Mr. Podesta's inbox for his most sensitive and potentially embarrassing correspondence, much of which has been posted on the WikiLeaks website. Additions to the collection on Thursday included three short

email exchanges between Mr. Podesta and Mr. Obama himself in the days leading up to his election in 2008.

Mr. Podesta's emails were first published by WikiLeaks earlier this month. The release came just days after James R. Clapper Jr., the director of national intelligence, and the Department of Homeland Security publicly blamed Russian officials for cyberattacks on the Democratic National Committee, in what they described as an effort to influence the American presidential election.

To date, no government officials have offered evidence that the same Russian hackers behind the D.N.C. cyberattacks were also behind the hack of Mr. Podesta's emails, but an investigation by the private security researchers determined that they were the same.

Threat researchers at Dell SecureWorks, an Atlanta-based security firm, had been tracking the Russian intelligence group for more than a year. In June, they reported that they had uncovered a critical tool in the Russian spy campaign. SecureWorks researchers found that the Russian hackers were using a popular link shortening service, called Bitly, to shorten malicious links they used to send targets fake Google login pages to bait them into submitting their email credentials.

The hackers made a critical error by leaving some of their Bitly accounts public, making it possible for SecureWorks to trace 9,000 of their links to nearly 4,000 Gmail accounts targeted between October 2015 and May 2016 with fake Google login pages and security alerts designed to trick users into turning over their passwords.

Among the list of targets were more than 100 email addresses associated with Hillary Clinton's presidential campaign, including Mr. Podesta's. By June, 20 staff members for the campaign had clicked on the short links sent by Russian spies. In June, SecureWorks disclosed that among those whose email accounts had been targeted were staff members who advised Mrs. Clinton on policy and managed her travel, communications and campaign finances.

Independent journalism.
More essential than ever.

Subscribe to the Times

Two security researchers who have been tracking the GRU's spearphishing campaign confirmed Thursday that Mr. Podesta was among those who had inadvertently turned over his Google email password. The fact that Mr. Podesta was among those breached by the GRU was first disclosed Thursday by Esquire and the Motherboard blog, which published the link Russian spies used against Mr. Podesta.

"The new public data confirming the Russians are behind the hack of John Podesta's email is a big deal," Jake Sullivan, Mrs. Clinton's senior policy adviser, said Thursday. "There is no longer any doubt that Putin is trying to help Donald Trump by weaponizing WikiLeaks."

The new release of Mr. Podesta's email exchange with Mr. Obama from 2008 made clear that Mr. Obama's team was confident he would win.

In one of the emails, Mr. Podesta wrote Mr. Obama a lengthy memo in the evening on Election Day recommending that he not accept an invitation from President George W. Bush to attend an emergency meeting of the Group of 20 leaders.

"Attendance alongside President Bush will create an extremely awkward situation," the memo said. "If you attempt to dissociate yourself from his positions, you will be subject to criticism for projecting a divided United States to the rest of the world. But if you adopt a more reserved posture, you will be associated not only with his policies, but also with his very tenuous global standing."

The White House did not respond to questions about the email.

Correction: October 22, 2016

An article on Friday about suspected email hacking by Russia's foreign intelligence service misstated the name of one organization that first disclosed that a presidential counselor, John D. Podesta, was among those whose accounts were breached. The blog is Motherboard, not VICE Motherload.

Nicole Perlroth reported from San Francisco, and Michael D. Shear from Washington.

Follow The New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on October 21, 2016, on page A14 of the New York edition with the headline: Private Security Group Says Russia Was Behind Hack of Clinton Campaign Chairman.

EXHIBIT D

NBCNEWS   SECTIONS ⌄   Q

NEWS > U.S. NEWS

WORLD   INVESTIGATIONS   CRIME & COURTS   ASIAN AMERICA   LATINO   NBCBLK

NEWS AUG 30 2016, 4:54 AM ET

Russians Hacked Two U.S. Voter Databases, Officials Say

by **ROBERT WINDREM**, **WILLIAM M. ARKIN** and **KEN DILANIAN**

SHARE   f   🐦   g+   💬

Hackers based in Russia were behind two recent attempts to breach state voter registration databases, fueling concerns the Russian government may be trying to interfere in the U.S. presidential election, U.S. intelligence officials tell NBC News.

The breaches included the theft of data from as many as 200,000 voter records in Illinois, officials say.

The incidents led the FBI to send a "flash alert" earlier this month to election officials nationwide, asking them to be on the lookout for any similar cyber intrusions.

One official tells NBC News that the attacks have been attributed to Russian intelligence agencies.

"This is the closest we've come to tying a recent hack to the Russian government," the official said.

That person added that "there is serious concern" that the Kremlin may be seeking to sow uncertainty in the U.S. presidential election process.

Voters cast their ballots at ChiArts High School on March 15 in Chicago, Illinois. 📷 Scott Olson / Getty Images

Two other officials said that U.S. intelligence agencies have not yet concluded that the Russian government is trying to do that, but they are worried about it.

They said the Russians have long conducted cyber espionage on political targets. The question now is whether they are moving into a covert intelligence operation designed to destabilize the U.S. political process.

The alert, first reported by Yahoo News, provided IP addresses associated with the hack attempts, though it did not mention Russia.

One of the IP addresses was involved in both breaches, the FBI alert said.

"The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected," the alert said.

The bulletin does not identify the targeted states, but officials told NBC News they were Illinois and Arizona. Illinois officials said in July that they shut down their state's voter registration after a hack. State officials said Monday the hackers downloaded information on as many 200,000 people.

State officials told the Chicago Tribune they were confident no voter record had been deleted or altered.

In Arizona, officials said, hackers tried to get in using malicious software but were unsuccessful. The state took its online voter registration down for nine days, beginning in late June, after malware was discovered on a county election official's computer. But the state concluded that the system was not successfully breached.

Those incidents led Homeland Security Secretary Jeh Johnson to host a call earlier this month with state election officials to talk about cybersecurity and election infrastructure.

Johnson said DHS isn't aware of any specific cyber threat against election-related networks, but he urged officials to examine how to better secure their systems, according to a summary of the call put out by the department.

U.S. intelligence officials have previously said Russian intelligence agencies were behind hacks into the Democratic National Committee and related organizations. There has been a long running debate among intelligence analysts about what Russia is up to.

Voting systems have not been considered "critical infrastructure," by the Department of Homeland Security, so they are not subject to federal government protections.

Independent assessments have found that many state and local voting system are extremely vulnerable to hacking. 🦚

　　ROBERT WINDREM　🐦 f ✉

WILLIAM M. ARKIN　🐦 ✉

　　KEN DILANIAN　🐦 ✉

TOPICS U.S. NEWS, INVESTIGATIONS, SECURITY, WORLD

FIRST PUBLISHED AUG 29 2016, 6:05 PM ET

⬇ **NEXT STORY** Trump's Victory Has Fearful Minorities Buying Up Guns

More to Explore   Sponsored Links by Taboola ▷

A Solution That Puts Snoring to Bed

My Snoring Solution

**Tiny Device Transforms Old Computer
into a Blazingly Fast PC**

Xtra-PC

**You Don't Need to Remember You
Passwords Anymore Thanks to This
Device**

Everykey

SPONSORED CONTENT   **MORE FROM NBC
NEWS**

Your Warrington
Grocery Store is
70% Mo... Blue Apron

Harry's Releases
New Blade. Keeps

EXHIBIT E

U.S. official: Hackers targeted voter registration systems of 20 states

In this June 5, 2015, file photo, the Homeland Security Department headquarters in northwest Washington. A Homeland Security Department official says hackers have targeted the voter registration systems of more than 20 states in recent months. FBI Director James Comey told lawmakers this week that the agency is looking "very, very hard" at **Russia**n hackers who may try to disrupt the U.S. election. (Susan Walsh / AP)

By **Tribune news services**

SEPTEMBER 30, 2016, 4:42 PM | WASHINGTON

Hackers have targeted the voter registration systems of more than 20 states in recent months, a Homeland Security Department official said Friday.

The disclosure comes amid heightened concerns that foreign hackers might undermine voter confidence in the integrity of U.S. elections. Federal officials and many cybersecurity experts have said it would be nearly impossible for hackers to alter an election's outcome because election systems are very decentralized and generally not connected to the internet.

ADVERTISING
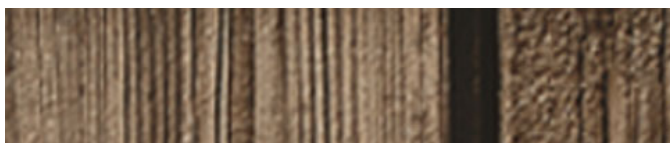
The official who described detecting the hacker activity was not authorized to speak publicly on the subject and spoke to The Associated Press on condition of anonymity. It was unclear, the official said, whether the hackers were foreign or domestic, or what their motives might be. ABC News earlier reported that more than 20 states were targeted.

The FBI last month warned state officials of the need to improve their election security after hackers targeted systems in Illinois and Arizona. FBI Director James Comey told lawmakers this week that the agency is looking "very, very hard" at Russian hackers who may try to disrupt the U.S. election.

Last month, Donald Trump, the GOP nominee for president, suggested that he feared the general election "is going to be rigged."

The Homeland Security Department has stepped up its outreach to states and localities, but it is up to them to ask for help. So far, 19 states have expressed interest in a general "cyber hygiene" scan of key websites — akin to ensuring that windows in a home are properly closed, according to another Homeland Security official directly involved in securing local elections who also was not authorized to speak publicly about ongoing efforts.

The FBI has detected a variety of "scanning activities" that are early indications of hacking, Comey told the House Judiciary Committee this week.

The FBI held a conference call on Friday with the local officials who run elections in the battleground state of Florida. Meredith Beatrice, a spokeswoman for Secretary of State Ken Detzner, called it an "informational call related to elections security," but a person on the call who was not authorized to discuss it and requested anonymity said authorities had seen evidence of someone probing a local elections website.

Homeland Security Secretary Jeh Johnson spoke to state election officials by phone last month, encouraging them to implement existing technical recommendations to secure their election systems and ensure that electronic voting machines are not connected to the internet.

DHS is offering states more comprehensive, on-site risk and vulnerability checks. Only four states have expressed interest in the assessment, and because the election is only weeks away, the department will likely only be able to conduct an assessment of one state before Election Day on Nov. 8, the official said.

Two of the hacking attempts involved efforts to mine data from the Arizona and Illinois voter registration systems, according to Kay Stimson, a spokeswoman for the National Association of Secretaries of State. She said in Arizona a hacker tried to probe voter registration data, but never infiltrated the system, while in Illinois hackers got into the system, but didn't manipulate any data.

These systems have "nothing to do with vote casting or counting," Stimson said in an email. "While it is theoretically possible to disrupt an election by infiltrating a voter registration system, their compromise would not affect election results" and there are system controls in place to catch any fraud.

Rep. Henry Johnson, D-Ga., introduced two bills earlier this month that would require voting systems be designated as critical infrastructure and limit purchases of new voting systems that don't provide paper ballots, among other measures. It's unlikely the bills will be passed before the election.

The Homeland Security Department is already considering designating voting systems as critical infrastructure in the future, though it is unlikely to happen before the election, the second official said.

A presidential directive released in 2013 details 16 sectors that are considered critical infrastructure, including energy, financial services, healthcare, transportation, food and agriculture, and communications. The designation places responsibilities on the Homeland Security secretary to identify and prioritize those sectors, considering physical and cyber threats. The secretary is also required to conduct security checks and provide information about emerging and imminent threats.

Associated Press

This article is related to: Jeh Johnson, James Comey

EXHIBIT F

theguardian

Senators call for declassification of files on Russia's role in US election

Eight members of Senate intelligence committee hint that government may still hold secret information 'concerning the Russian government'

The eight senators did not directly accuse the Russian government or Donald Trump of wrongdoing. Photograph: Timothy A Clary/AFP/Getty Images

Spencer Ackerman in New York

Thursday 1 December 2016 11.07 EST

All of the Democratic and Democratic-aligned members of the Senate intelligence committee have hinted that significant information about Russian interference in the US presidential election remains secret and ought to be declassified.

The eight senators, including the incoming ranking member Mark Warner of Virginia, wrote to Barack Obama to request he declassify relevant intelligence on the election. They did not directly accuse the Russian government or President-elect Donald Trump, a Republican, of wrongdoing in the letter.

"We believe there is additional information concerning the Russian government and the US election that should be declassified and released to the public. We are conveying specifics through classified channels," wrote Warner and his colleagues Ron Wyden of Oregon, Martin Heinrich of New Mexico, Mazie Hirono of Hawaii, Barbara Mikulski of Maryland and independent Angus King of Maine.

Jack Reed of Rhode Island, an honorary and non-voting member of the committee due to his seat as ranking member of the Senate armed services committee, also signed the letter, which was dated Tuesday and publicly released on Wednesday. No Republican joined the declassification call.

The outgoing ranking Democrat, Dianne Feinstein of California, signed the classified version of the letter sent to Obama.

Neither the terse letter nor discussions with sources on Capitol Hill detailed the particular intelligence concerning the Russians, its strength or its impact on the outcome of the election. Thus far, no credible evidence of vote fraud or electoral malfeasance exists, despite an evidence-free claim from Trump himself.

A spokesman for Wyden, Keith Chu, said the senator believed the intelligence needed to be declassified "immediately", as it was in the "national interest that the American public should see it".

It is understood this is the first declassification request by eight senators in at least twelve years.

On 7 October, the US director of national intelligence and the secretary of homeland security took the rare step of directly accusing Russia's "senior-most" officials of ordering the breach of the Democratic National Committee's digital networks. Director James Clapper and Secretary Jeh Johnson accused the Russians of attempting to "interfere" in the US election, something the Obama administration had previously suggested but did not allege publicly.

The FBI has acknowledged investigating such interference, but has reportedly not established any link to Trump or his campaign. Two US officials have told the Guardian that the FBI was reluctant to sign off on Clapper and Johnson's public allegation.

Yet Harry Reid, the outgoing Democratic Senate leader, asserted without evidence in October that the FBI director, James Comey, "possess[es] explosive information about close ties and coordination between Donald Trump, his top advisers, and the Russian government".

Unusually for any presidential nominee, and particularly for a Republican, Trump has exhibited a warmth toward the Russian president, Vladimir Putin, that has prompted a widespread expectation Trump will tilt US foreign policy toward Russia. Trump and Putin spoke soon after Trump's electoral victory in a phone call heralded by the Kremlin.

There was no immediate comment from the White House or Clapper's office as to whether Obama would order the declassification or whether the intelligence agencies even support such a move.

Since you're here ...

... we have a small favour to ask. More people are reading the Guardian than ever but far fewer are paying for it. And advertising revenues across the media are falling fast. So you can see why we need to ask for your help. The Guardian's independent, investigative journalism takes a lot of time, money and hard work to produce. But we do it because we believe our perspective matters – because it might well be your perspective, too.

Fund our journalism and together we can keep the world informed.

Become a Supporter
Make a contribution
More news

Topics

US elections 2016 Russia US politics US Senate

Save for later Article saved
Reuse this content

EXHIBIT G

Official website of the Department of Homeland Security

Contact Us | Quick Links | Site Map | A-Z Index
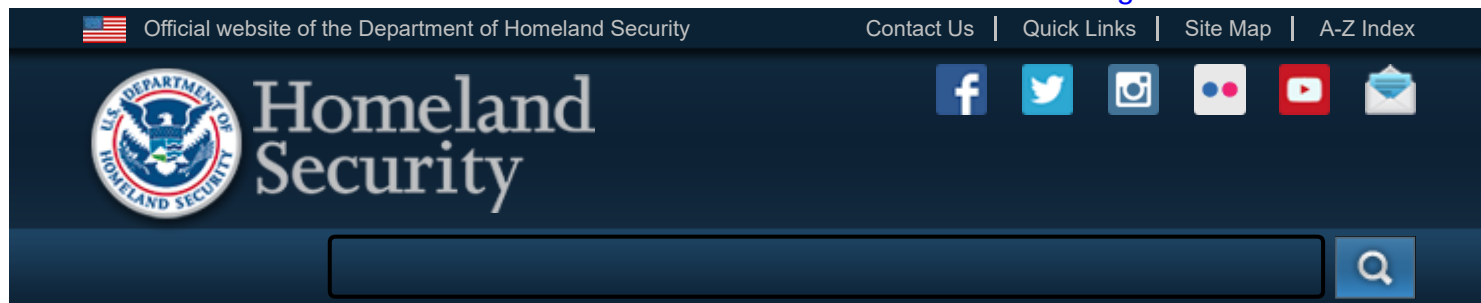
Homeland Security

Share / Email

Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security

Release Date: October 7, 2016

For Immediate Release
DHS Press Office
Contact: 202-282-8010

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts.

These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber "hygiene" scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share

information, and provide additional resources to state and local officials.

# # #

Last Published Date: October 7, 2016

EXHIBIT H

Passcode
Modern field guide to security and privacy

WORLD | PASSCODE

Ukraine election narrowly avoided 'wanton destruction' from hackers (+video)

A brazen three-pronged cyber-attack against last month's Ukrainian presidential elections has set the world on notice – and bears Russian fingerprints, some say.

By **Mark Clayton**, Staff writer ▼ | JUNE 17, 2014

Save for later

David Mdzinarishvili/Reuters | View Caption

A three-pronged wave of cyber-attacks aimed at wrecking Ukraine's presidential vote – including an attempt to fake computer vote totals – was narrowly defeated by government cyber experts, Ukrainian officials say.

The still little-known hacks, which surfaced May 22-26, appear to be among the most dangerous cyber-attacks yet deployed to sabotage a national election – and a warning shot for future elections in the US and abroad, political scientists and cyber experts say.

National elections in the Netherlands, Norway, and other nations have seen hackers probe Internet-tied election systems, but never with such destructive abandon, said experts monitoring the Ukraine vote.

> Recommended: **How much do you know about cybersecurity? Take our quiz.**

"This is the first time we've seen a cyber-hacktivist organization act in a malicious way on such a grand scale to try to wreck a national election "

Popular Now

1. Does this crab have the most crushing claws?
2. 7 recipes for green bean casserole
3. Does your dog remember what you did?
4. With Nikki Haley pick, Trump sends different message
5. Why Hillary Clinton lost the white women's vote

Follow Passcode

Passcode covers security and privacy in the digital age. Sign up below to stay up to date with Passcode news, columnists, and upcoming events.Read more about us.

E-mail address   SIGN-UP

Michael B. Farrell
Passcode Editor | Michael is an editor and writer based in Boston.

Sara Sorcher
Passcode Deputy Editor | Sara covers security and privacy policy from DC.

Jack Detsch
Staff writer | Jack is the Mark Clayton Fellow in Cybersecurity

Case 1:17-cv-02989-AT   Document 260-2   Filed 08/07/18   Page 79 of 83

malicious way on such a grand scale to try to wreck a national election, says Joseph Kiniry, an Internet voting systems cyber-security expert. "To hack in and delete everything on those servers is just pillaging, wanton destruction."

That wanton destruction began four days ahead of the national vote, when CyberBerkut, a group of pro-Russia hackers, infiltrated Ukraine's central election computers and deleted key files, rendering the vote-tallying system inoperable. The next day, the hackers declared they had "destroyed the computer network infrastructure" for the election, spilling e-mails and other documents onto the web as proof.

A day later, government officials said the system had been repaired, restored from backups, and was ready to go. But it was just the beginning.

Only 40 minutes before election results were to go live on television at 8 p.m., Sunday, May 25, a team of government cyber experts removed a "virus" covertly installed on Central Election Commission computers, Ukrainian security officials said later.

If it had not been discovered and removed, the malicious software would have portrayed ultra-nationalist Right Sector party leader Dmytro Yarosh as the winner with 37 percent of the vote (instead of the 1 percent he

actually received) and Petro Poroshenko (the actually winner with a majority of the vote) with just 29 percent, Ukraine officials told reporters the next morning.

Curiously, Russian Channel One aired a bulletin that evening declaring Mr. Yarosh the victor with 37 percent of the vote over Mr. Poroshenko with 29 percent, Ukraine officials said.

"Offenders were trying by means of previously installed software to fake election results in the given region and in such a way to discredit general results of elections of the President of Ukraine," the Ukrainian Security Service (SBU) said in a statement.

Still, there was more to come.

In the wee hours of the morning after polls closed, as results flowed in from Ukrainian election districts, Internet links feeding that data to the vote tally system were hit with a barrage of fake data packets – known as distributed denial of service (DDoS) attacks. So from about 1 to 3 a.m. on May 26, election results were blocked, delaying the finally tally until the early

TEST YOUR KNOWLEDGE | How much do you know about cybersecurity? Take our quiz.
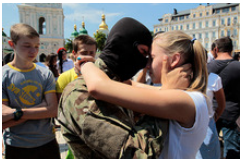
IN PICTURES | Ukraine: 10 years in 30 images

▶

VIDEO | Ukraine election results

Paul F. Roberts
Correspondent | Paul covers critical infrastructure and the Internet of Things.

Jaikumar Vijayan
Correspondent | Jaikumar is an award-winning technology reporter.

Nadya T. Bliss
Columnist | Nadya directs the Global Security Initiative at Arizona State Uni...

Lorrie Faith Cranor
Columnist | Lorrie is chief technologist at the Federal Trade Commission

Dan Geer
Columnist | Dan is chief information security officer for In-Q-Tel.

Jason Healey
Columnist | Senior Research Scholar, Columbia University SIPA

Sascha Meinrath
Columnist | Sascha founded the Open Technology Institute.

Lysa Myers
Columnist | Lysa Myers is a security researcher at ESET.

Bruce Schneier
Columnist | Bruce is a noted cryptographer and security expert.

Evan Selinger
Columnist | Evan is a philosophy professor at Rochester Institute of Technology.

Melanie Teplinsky
Columnist | Melanie teaches information privacy law at American University.

Nicole Wong
Columnist | Nicole served as deputy chief technology officer at the White House.

morning, a preliminary report by international election observers recounted.

An analysis of the DDoS attack by Arbor Networks, a Burlington, Mass., cyber-security company, ties it to CyberBerkut.

In the end, international observers declared Ukraine's vote "a genuine election." But US researchers say it's clear that Ukraine dodged a major cyber-bullet.

"We've seen vote fraud before in Ukraine, including a rigged computer system in 2004," says Peter Ordeshook, a California Institute of Technology political scientist. "But this wasn't an effort to steal the election outcome, so much as to steal the election itself – by entirely discrediting it in the eyes of key segments of the population in Ukraine and in Russia, too."

While it was well understood across most of Ukraine and internationally that the far-right candidate Yarosh had little political support, the faked results would have lent credibility to Russian-inspired accounts that the popular revolt last fall against the Ukraine government was fomented by ultra-nationalists.

"In that light, the cyber fakery looks incredibly clumsy from the outside because no one there would have believed it," Dr. Ordeshook says. "But these faked results were geared for a specific audience in order to feed the Russian narrative that has claimed from the start that ultra-nationalists and Nazis were behind the revolution in Ukraine."

If the virus with the faked computer results had not been discovered, it would have fomented unrest across the volatile ethnic-Russian Donetsk region now under the shadow of Russian forces on the border with Ukraine, he says. Such spurious results also would have undermined the credibility of the new Ukraine government and could have paved the way for Russian military action, say political scientists who monitor Ukraine elections.

The Ukraine hack is a stark warning for the US and other democracies that use the Internet for tabulation and even direct voting, election security experts say. One clear lesson, they say, is to always have paper ballots to back up election results – like Ukraine – and to avoid Internet voting.

"The Ukraine attack story demonstrates there is no shortage of methods which a determined adversary will make use of to sabotage an election," says Pamela Smith, president of the Verified Voting Foundation, a US group that has researched US election systems security.

In the runup to the election, President Obama on May 2 warned Russia not to interfere or the US "will not have a choice but to move forward with additional, more severe sanctions."

Since then, US officials appear reluctant to make too much of the attacks. References to the cyber-attacks have been brief and oblique. With anonymity cloaking cyber-attacks across the Internet, it's difficult to tell

anonymity cloaking cyber-attacks across the Internet, it's difficult to tell how deeply involved Russia's government might have been.

Ukraine experienced "cyber-attacks on the Central Election Commission of the kind that generally would require outside support," Victoria Nuland, assistant secretary of State for European affairs, acknowledged in a May 27 interview on the Charlie Rose show. Mark Green, a former congressman, said in Senate testimony June 6 that he had been told by a US diplomat of a failed Russian cyber-attack on the election.

Ukrainian officials have been unabashed in throwing blame at Russia, saying that arrests were made in the case, although no names have yet been made public.

"It was prepared in advance and stored on Russian (Internet) re-sources," Volodymyr Zverev, head of the Ukraine's Administration of Public Service of Special Communication and Protection of Information said of the malware that was intended to deliver the fake election results, according to Interfax-Ukraine. "They wanted to, and made the preparations, but they did not succeed."

While Russian hacktivists appear to be linked to at least some of the attacks, not everyone agrees the Russian government had a hand in the most devious element. Internet security expert Mr. Kiniry, for instance, says there is no solid proof yet to back the Ukrainian government claim of a virus carrying fake election results.

Others say Russia's paw prints are all over the attack.

"Did Russia attempt to sway the Ukrainian Presidential Election? I honestly don't know the answer to that," says Jeffery Stutzman, CEO of Red Sky Alliance, a cyber-security group in New Hampshire.

But, he adds, "the idea that these guys were trying to poison the election result by compromising the election commission computers is amazing to me – and this coincidence with the Russian channel showing the same fake results – is just too much. If it walks like a duck and quacks like one, maybe it's a duck." ▮
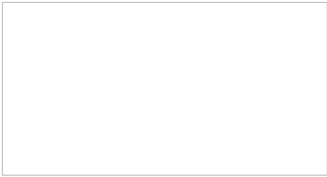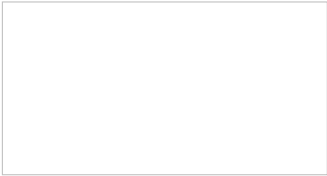
Next up

PASSCODE

How much do you know about cybersecurity? Take our quiz.
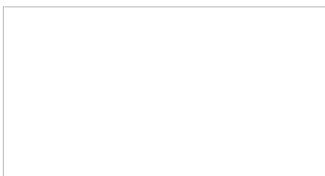
Major cyber-assaults on Ukraine, then Moscow, on eve of Crimea vote (+video)

How Iran duped high-ranking US officials with fake website

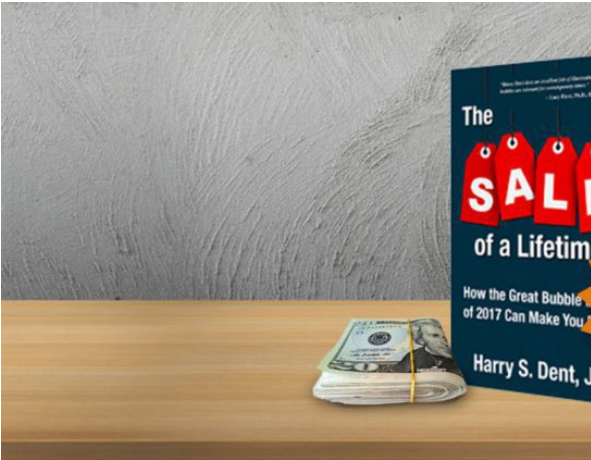US indicts five in China's secret 'Unit 61398' for cyber-spying on US firms (+video)

Share   Tweet   E-mail   More   Print/Reprints

How the Great Bubble Burst of 2017 Can Make You

Global Galleries   Latest News   Doing Good

Photos of the day 11/23

Does your dog remember what you did?

DIFFERENCE MAKER   He's championed cleanup of the Chesapeake Bay for four decades

The **CHRISTIAN SCIENCE**
MONITOR®

STAY CURRENT. GO FAR.
DISCOVER THE MONITOR DIFFERENCE

f   🐦 g+

ABOUT | CONTACT US | SUBSCRIBE | E-READERS | ADVERTISE WITH US | CAREERS | FIND US ONLINE
CONTENT MAP | TEXT | CORRECTIONS | REPRINTS & PERMISSIONS | MULTIMEDIA | A CHRISTIAN SCIENCE PERSPECTIVE