NOTICE OF RECOUNT FOR THE
OFFICE OF PRESIDENT OF THE UNITED STATES
ST. CROIX COUNTY – NOVEMBER 8, 2016 GENERAL ELECTION

TO: ALL CANDIDATES ON THE BALLOT FOR THE OFFICE OF PRESIDENT OF THE UNITED STATES AND OTHER INTERESTED PERSONS

FROM: CINDY CAMPBELL, ST. CROIX COUNTY CLERK

SUBJECT: RECOUNT OF THE VOTES CAST FOR THE OFFICE OF PRESIDENT OF THE UNITED STATES FOR THE STATE OF WISCONSIN, ST. CROIX COUNTY IN THE NOVEMBER 8, 2016 GENERAL ELECTION

DATE: NOVEMBER 29, 2016

A recount of the votes cast at the November 8, 2016 General Election for the Office of President of the United States will begin at the time and location set forth below:

ST. CROIX COUNTY GOVERNMENT CENTER
COUNTY BOARD ROOM
1101 CARMICHAEL ROAD, HUDSON, WISCONSIN
DECEMBER 1, 2016 -- 9:00 A.M.

A copy of the recount petition is attached. This notice is given pursuant to § 9.01(2), Wis. Stats.

You have the right to be present and to be represented by counsel to observe and challenge the votes cast and the board of canvassers' decisions at the election.

A public test of the optical scan equipment will be conducted during the recount.

In Re: The Election for President of the United States	Verified Petition for Recount

Petitioner Jill Stein alleges and shows to the Wisconsin Elections Commission:

1. That Petitioner was a candidate for the office of the President of the United States in an election held on November 8, 2016;

2. That Petitioner is informed and believes that an irregularity has occurred affecting all wards in Wisconsin in the counting and return of votes cast for the office of President;

3. The Petitioner is informed and believes that:

    a. In August 2016, it was widely reported that foreign operators breached voter registration databases in at least two states and stole hundreds of thousands of voter records.

    b. Around that time, hackers infiltrated the e-mail systems of the Democratic National Committee and a campaign official for Democratic presidential candidate Hillary Clinton. These e-mails were then published online.

    c. On October 7, 2016, the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence on Election Security issued a joint statement regarding these breaches. The statement reads, in pertinent part, as follows: "The U.S. Intelligence Community (USIC) is confident" that there have been "recent compromises of e-mails from US persons and institutions, including from US political organizations." It also states that "[t]hese thefts and disclosures are intended to interfere with the US election process" and that "similar tactics and techniques [have been used] across Europe and Eurasia . . . to influence public opinion there." In the statement, DHS urges state election officials "to be vigilant and seek cybersecurity assistance" from that agency in preparation for the presidential election.

    d. Wisconsin uses two forms of electronic voting machines—optical scan and direct-recording electronic (DRE)—both of which are susceptible to compromise. For the last decade, computer scientists have warned about the vulnerabilities of these machines, including that they can be breached without detection and even after certain security measures are put in place.

e. In Wisconsin, there is evidence of voting irregularities in the 2016 presidential election that indicate potential tampering with electronic voting systems. Specifically, there was a significant increase in the number of absentee voters as compared to the last general election. This significant increase could be attributed to a breach of the state's electronic voter database.

f. The well-documented and conclusive evidence of foreign interference in the presidential race before the election, along with the irregularities observed in Wisconsin, call into question the results and indicate the possibility that widespread breach occurred.

g. A hand count of paper ballots, including those used in optical scan machines, and a review of the paper record from DRE machines are necessary to make this determination. Without utilizing these methods, a recount would not exclude the possibility of a breach that resulted in a miscounting of votes; and

4. Attached as Exhibit 1, and incorporated fully herein, is the affidavit of J. Alex Halderman, Ph.D., 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, that details the basis for of my belief for the statements set forth in paragraph 3 above.

Wherefore: Petitioner requests a hand recount of all ballots in all wards in the State of Wisconsin pursuant to Wis. Stat. § 9.01.

Dated this 25th day of November, 2016.

Petitioner Jill Stein

I, Jill Stein, being first duly sworn, on oath, state that the matters contained in the above petition are known to me to be true except for those allegations stated on information and belief, which I believe to be true.

Jill Stein

Petitioner Jill Stein

Subscribed and sworn to before me this 25th day of November, 2016.

Notary Public

My Commission Expires 09/10/2021

On this 25 day of November, 2016, before me, the undersigned notary public, personally appeared Jill Stein (name of document signer), proved to me through satisfactory evidence of identification, which were MA Drivers License, to be the person whose name is signed above, and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of his/her knowledge and belief.

(signature of notary public) Michael J. Damon (printed name of notary public)

09 / 10 / 2021 (my commission expires)

MICHAEL J. DAMON
Notary Public, Commonwealth of Massachusetts
My Commission Expires September 10, 2021

Exhibit 1

EXHIBIT 1

In Re: The Election for President of the United States	Affidavit in Support of Petition of Jill Stein for Recount

AFFIDAVIT OF J. ALEX HALDERMAN

J. ALEX HALDERMAN, being duly sworn, deposes and says the following under penalty of perjury:

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.

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, data privacy, and electronic voting.

4. I have published peer-reviewed research analyzing the security of electronic voting systems used in Wisconsin, other U.S. states, and other countries. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom" review of the state's electronic voting systems. 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.

5. I have published numerous other peer-reviewed papers in these areas of research. My full curriculum vitae, including a list of honors and awards, research projects, and publications, is attached as Exhibit A.

Context: Cyberattacks and the 2016 Presidential Election

6. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, 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 B and C. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. Exhibit D. The Department of Homeland Security has stated that senior officials in the Russian government commissioned these attacks. Exhibit E. Attackers attempted to breach election offices in more than 20 other states. Exhibit F.

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

8. If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices well in advance to find ways to break

into the computers. Next, closer to the election, when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines into some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. This malware would likely be designed to remain inactive during pre-election tests, perform its function during the election, and then erase itself after the polls closed. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling.

The Vulnerability of American Voting Machines to Cyberattack

9. As I and other experts have repeatedly documented in peer-reviewed and state-sponsored research, American voting machines have serious cybersecurity problems. 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. As I have demonstrated in laboratory tests, in just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote.[1]

10. Whether voting machines are connected to the Internet is irrelevant. Shortly before each election, poll workers copy the ballot design from a regular desktop computer in a government office and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers

---

[1] A video documenting this result is publicly available at https://youtu.be/aZws98jw67g.

infect that computer, they can spread vote-stealing malware to every voting machine in the area. Technically sophisticated attackers can accomplish this with ease.

11. While the vulnerabilities of American voting machines have been known for some time, states' responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Wisconsin, continue to use out-of-date machines that are known to be insecure.

Examining the Paper Record Is the Only Way to Ensure the Integrity of the Result

12. Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks.

13. One explanation for the results of the 2016 presidential election is that cyberattacks influenced the result. This explanation is plausible, in light of other known cyberattacks intended to affect the outcome of the election; the profound vulnerability of American voting machines to cyberattack; and the fact that a skilled attacker would leave no outwardly visible evidence of an attack other than an unexpected result.

14. The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, to count the paper ballots and paper audit trail records, and review the voting equipment, to ensure that the votes cast by actual voters match the results determined by the computers. For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, must occur. Using the electronic equipment to conduct the recount, even after first

evaluating the machine through a test deck, is insufficient. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests. For votes cast on electronic voting machines, the paper audit trail records must be counted, since the electronic records stored in the machines could have been manipulated in an attack. Voting equipment that might yield forensic evidence of an attack includes the voting machines, removable media, and election management system computers. Paper ballots, paper audit trails, and voting equipment will only be examined in this manner if there is a recount.

15. A recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference. It will also set a precedent that may provide an important deterrent against cyberattacks on future elections.

This affidavit was executed on the 25th day of November, 2016 in Buckingham, Pennsylvania.

J. ALEX HALDERMAN

Sworn to before me this 25th day of November, 2016.

Victoria L. Child

Notary Public

My Commission Expires: November 24, 2019

Commonwealth of Pennsylvania
NOTARIAL SEAL
Victoria L. Child, Notary Public
Buckingham Twp., Bucks County
My commission expires
November 24, 2019

Exhibit A

J. Alex Halderman

Professor, Computer Science and Engineering
University of Michigan

2260 Hayward Street
Ann Arbor, MI 48109 USA
(*mobile*) +1 609 558 2312
jhalderm@eecs.umich.edu

J.AlexHalderman.com

November 4, 2016

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, digital rights management, computer forensics, ethics, and cybercrime. I'm also interested in the interaction of technology with law, regulatory policy, and international affairs.

Selected Projects

'16: Let's Encrypt HTTPS certificate authority
'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)

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

Honors and Awards

- 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 his/her College, and a teacher whose scholarly integrity pervades his/her service and the profession of Engineering")
- Morris Wellman Faculty Development Assistant Professorship (2015)
  ("awarded to a junior faculty member to recognize outstanding contributions to teaching and research")
- **Best Paper Award** of the 14th ACM Internet Measurement Conference
  for "The Matter of Heartbleed" (2014)
- **Best Paper Award** of the 21st USENIX Security Symposium
  for "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" (2012)
- Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies
  for "Telex: Anticensorship in the Network Infrastructure" (2012)
- John Gideon Memorial Award from the Election Verification Network
  for contributions to election verification (2011)
- **Best Student Paper** of the 17th USENIX Security Symposium
  for "Lest We Remember: Cold Boot Attacks on Encryption Keys" (2008)
- Pwnie Award in the category of "Most Innovative Research"
  for "Lest We Remember: Cold Boot Attacks on Encryption Keys," Black Hat 2008
- Charlotte Elizabeth Procter Honorific Fellowship, Princeton University (2007)
  ("awarded in recognition of outstanding performance and professional promise, and represents high commendation from the Graduate School")
- National Science Foundation Graduate Research Fellowship (2004–2007)

- **Best Paper Award** of the 8th International Conference on 3D Web Technology for "Early Experiences with a 3D Model Search Engine" (2003)
- Princeton Computer Science Department Senior Award (2003)
- Accenture Prize in Computer Science, Princeton University (2002)
- Martin A. Dale Summer Award, Princeton University (2000)
- USA Computing Olympiad National Finalist (1996 and 1997)

Refereed Conference Publications

[1] **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
To appear in *Proc. 24th Network and Distributed Systems Symposium* (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[2] **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
To appear in *Proc. 24th Network and Distributed Systems Symposium* (NDSS), February 2017.
Acceptance rate: 16%, 68/423.

[3] **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
To appear in *Proc. 14th IEEE Conference on Privacy, Security, and Trust* (PST), December 2016.

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

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

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

[7] **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.

[8] **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.

[9] **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.

[10] **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.

[11] **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.

[12] **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.

[13] **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.

[14] **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.

[15] **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.

[16] **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.

[17] **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.

[18] **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.

[19] **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.

[20] **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.

[21] **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.

[22] **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.

[23] **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.

[24] **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.

[25] **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.

[26] **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.

[27] **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.

[28] **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.

[29] **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.

[30] **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.

[31] **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.

[32] **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.

[33] **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.

[34] **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.

[35] **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.

[36] **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.

[37] **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.

[38] **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.

[39] **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

[40] **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, 2016.

Journal Publications

[41] **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.

[42] **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

[43] **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.

[44] **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.

[45] **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.

[46] **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.

[47] **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.

[48] **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.

[49] **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.

[50] **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.

[51] **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.

[52] **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.

[53] **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.

[54] **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.

[55] **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.

[56] **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.

[57] **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

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

[59] **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.

[60] **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.

[61] **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.

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

[63] **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.

[64] **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.

[65] **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.

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

[67] **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

[68] **Request for DMCA Exemption: Games with Insecure DRM and Insecure DRM Generally**
Comment 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.)

[69] **Request for DMCA Exemption for Audio CDs with Insecure DRM**
Comment 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

[70] **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.

[71] **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

- **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 Legacy of Export-grade Cryptography in the 21st Century.** Invited talk, Summer school on real-world crypto and privacy, Croatia, June 9, 2016.

– **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web.** Invited talk, Cubaconf, Havana, April 25, 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)

- Moderator: **Apple & the FBI: Encryption, Security, and Civil Liberties.** Panelists: Nate Cardozo and Barbara McQuade. U-M Dissonance Speaker Series, April 12, 2016.
- Moderator: **Privacy, IT Security and Politics.** Panelists: Ari Schwartz and David Sobel. U-M ITS SUMIT_2015, Oct. 22, 2015.
- Panelist: **The Future of E-Voting Research.** 5th International Conference on E-Voting and Identity (VoteID), Bern, Switzerland, Sep. 4, 2015.
- Moderator: **Panel on Research Ethics.** 24th USENIX Security Symposium, Washington, D.C., August 13, 2015.
- Panelist: **Theories of Privacy in Light of "Big Data."** Michigan Telecommunications and Technology Law Review Symposium on Privacy, Technology, and the Law, University of Michigan Law School, Feb. 21, 2015.
- Panelist: **Measuring Privacy**. Big Privacy symposium, Princeton University CITP, Apr. 26, 2013 [moderator: Ed Felten].

- Panelist: **Civil Society's Challenge in Preserving Civic Participation**. The Public Voice workshop: Privacy Rights are a Global Challenge, held in conjunction with the 34th International Conference of Data Protection and Privacy Commissioners, Punta del Este, Uruguay, Oct. 22, 2012 [moderator: Lillie Coney].
- Panelist: **Election Technologies: Today and Tomorrow**. Microsoft Faculty Summit (Redmond), July 17, 2012 [moderator: Josh Benaloh].
- Panelist: **Is America Ready to Vote on the Internet?** CSPRI Seminar, George Washington University (Washington, D.C.), May 16, 2012 [moderator: Lance Hoffman].
- Panelist: **Technical Methods of Circumventing Censorship**. Global Censorship Conference, Yale Law School, Mar. 31, 2012.
- Panelist: **Internet Voting**. RSA Conference (San Francisco), Mar. 1, 2012 [moderator: Ron Rivest].
- Panelist: **The Law and Science of Trustworthy Elections**. Association of American Law Schools (AALS) Annual Meeting, Jan. 5, 2012 [moderator: Ron Rivest].
- Panelist: **Connecticut Secretary of State's Online Voting Symposium** (New Britain, CT), Oct. 27, 2011 [moderator: John Dankosky].
- Panelist: **CS Saves the World**. Michigan CSE Mini-symposium, Mar. 19, 2011 [moderator: Prabal Dutta].
- 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. in progress; NSF Graduate Research Fellowship)
- Zakir Durumeric (Ph.D. in progress; Google Ph.D. Fellowship in Computer Security)
- Travis Finkenauer (M.S. 2016; went on to security position at Juniper Networks)
- Eric Wustrow (Ph.D. 2016; went on to tenure track faculty position at U. Colorado, Boulder)
- James Kasten (Ph.D. 2015; went on to software engineering position at Google)
- Scott Wolchok (M.S. 2011; went on to software engineering position at Facebook)

Post Docs

- Colleen Swanson (2014–15)

Doctoral Committees

- Denis Bueno (C.S. P.D. expected 2016, Michigan)
- Eric Crockett (C.S. Ph.D expected 2016, Georgia Tech)
- 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

- 2016: Ben Burgess, Noah Duncan
- 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: Fall 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 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–present)
- CSE Undergraduate Program Advising (CS/ENG) (2011–present)
- Faculty Senate, Rules Committee of the Senate Assembly (member, 2011–12)
- CSE Graduate Admissions Committee (member, 2010–11)
- CSE Graduate Committee (member, 2009–10)

Broader Impact of Selected Projects

- **Let's Encrypt: A Certificate Authority to Encrypt the Entire Web** (2016)
  Co-founded a new HTTPS certificate authority to provide free, browser-trusted, automatically validated certificates for all domains. Developed in partnership with EFF and Mozilla, Let's Encrypt has helped secure millions of websites and is now issuing certificates at a greater rate than all other CAs combined.
- **The Logjam Attack and Weak Practical Use of Diffie-Hellman** (2015)
  Introduced Logjam, a practical attack on TLS that affected nearly 10% of popular HTTPS websites. Our results suggest that state-level attackers can break 1024-bit Diffie-Hellman, providing the first parsimonious explanation for how NSA is decrypting widespread VPN traffic, as revealed by Snowden.
- **Security Analysis of the Estonian Internet Voting System** (2014)
  Led the first rigorous security review of world's most significant Internet voting system. Based on code review, laboratory testing, and in-person observation, our study revealed significant shortcomings that could allow state-level attackers to upset national elections.
- **ZMap Internet-Wide Scanner Open-Source Project** (2013)
  Created ZMap, a network probing tool designed for Internet-wide measurement research that achieves up to 10,000× better performance than earlier tools. Now a thriving open-source project, ZMap is available in major Linux distros. We also maintain Scans.io, a public scan data repository.
- **Detection of Widespread Weak Keys in Network Devices** (2012)
  After conducting the largest Internet-wide survey of HTTPS and SSH hosts, we uncovered serious flaws in cryptographic public key generation affecting millions of users. We disclosed vulnerabilities to more than 60 network device makers and spawned major changes to the Linux random number generator.
- **The Telex Anticensorship System** (2011)
  Invented a fundamentally new approach to circumventing state-level Internet censorship, based on placing anticensorship technology into core network infrastructure outside the censoring country. Prototype attracted over 100,000 users, mainly in China. Now testing next-gen. schemes at partner ISP.
- **Attacking Washington, D.C.'s Internet Voting System** (2010)
  Participated in the first public security trial of an Internet voting system set to be deployed in a real election. We found serious flaws that allowed us to change all votes without detection. This led to the system being scrapped, and the widespread media coverage has altered the debate on Internet voting.

- **Analysis of India's E-Voting System** (2010)
  Participated in the first independent security review of the electronic voting machines used by half a billion voters in India. The flaws uncovered in our work were front-page news. After arresting my coauthor and threatening to deport me, officials eventually moved to adopt a paper trail nationwide.
- **Green Dam Youth Escort Censorware** (2009)
  Uncovered security problems and copyright infringement in client-side censorship software mandated by the Chinese government. Findings helped catalyze popular protest against the program, leading China to reverse its policy requiring installation on new PCs.
- **Cold-Boot Attacks** (2008)
  Developed the "cold boot" attack against software disk encryption systems, which altered widespread thinking on security assumptions about the behavior of RAM, influenced computer forensics practice, and inspired the creation of a new subfield of theoretical cryptography.
- **California "Top-to-Bottom" Review** (2007)
  Helped lead the California Secretary of State's "top-to-bottom" review of electronic voting machines, the first public review of this technology by any state. Our reports led California to discontinue use of highly vulnerable touch-screen voting systems and altered the course of election technology in the U.S.
- **DMCA Exemptions for Security** (2006 and 2010)
  Worked with legal teams to successfully petition the U.S. Copyright Office to create exemptions to the Digital Millennium Copyright Act (which prohibits circumventing DRM) in order to allow the public to investigate and repair security problems caused by certain DRM. One of only six exemptions granted.
- **Sony DRM Rootkit** (2005)
  Discovered dangerous security side-effects in the design of copy protection software used for music CDs. Resulted in the recall of millions of discs, class action lawsuits, and an investigation by the U.S. Federal Trade Commission in which I served as a technical expert on DRM's harm to consumers' security.
- **The Art of Science** (2004)
  Co-founded an interdisciplinary art competition at Princeton University that showcases images and videos produced in the course of scientific research as well as creative works that incorporate tools and ideas from science. Following international attention, the concept has spread to many other campuses.

Outreach and Press Coverage

I'm a regular contributor to **Freedom-to-Tinker**, a blog hosted by Princeton's CITP. My posts discuss current issues in security and public policy or announce new research results, aiming to communicate findings to nonspecialists.

I'm happy to speak to the press when I believe the topic is important for the public to understand. Much of my research has received significant media attention.

Selected media outlets *Television:* CNN, Fox News, CBS Evening News, NBC Nightly News, MSNBC, CNBC, MTV, Al Jazeera, C-SPAN. *Radio:* NPR News, NPR Science Friday, BBC World Service, The Diane Rehms Show. *Print*: The New York Times, LA Times, USA Today (front page profile), The Wall Street Journal, Washington Post, Boston Globe, Times of India, Time, Fortune, Harpers (incl. Harpers Index), The Atlantic; The Economist, New Scientist, MIT Tech Review, Businessweek, Redbook, PC Magazine, Playboy (long-form profile). *Online*: Hacker News (dozens of top stories), Slashdot (>40 stories), Reddit (top of front page), BoingBoing, CNET News, Wired News, TechNewsDaily, Science Daily, Gizmodo, TechDirt, Ars Technica, The Register, Huffington Post, Politico, The Drudge Report, and hundreds more.

References

Edward W. Felten
Professor
Princeton University
ACM Fellow, NAE Member
felten@cs.princeton.edu

Farnam Jahanian
Provost
Carnegie Mellon University
AAAS, ACM, & IEEE Fellow
farnam@andrew.cmu.edu

Ronald L. Rivest
Professor
MIT
A.M. Turing Award Winner
rivest@mit.edu

Michael Bailey
Associate Professor
UIUC
mdbailey@illinois.edu

Matt Blaze
Professor
University of Pennsylvania
mab@crypto.com

Avi Rubin
Professor
Johns Hopkins University
rubin@jhu.edu

Doug Tygar
Professor
U. C. Berkeley
doug.tygar@gmail.com

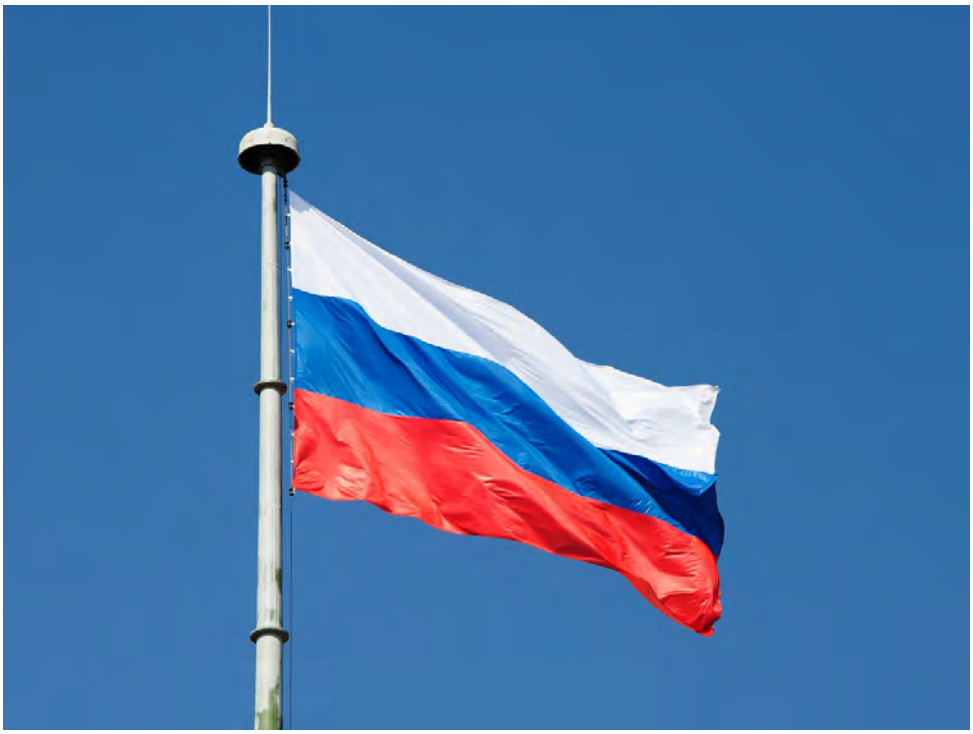
Dan Wallach
Professor
Rice University
dwallach@cs.rice.edu

David Wagner
Professor
U. C. Berkeley
daw@cs.berkeley.edu

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.

© 2016 The New York Times Company

Exhibit D

advertisement

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

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

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

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

Harry's Releases New Blade, Keeps

MORE FROM NBC NEWS

ABOUT US CAREERS CONTACT PRIVACY POLICY NEW TERMS OF SERVICE NBCNEWS.COM SITE MAP ADVERTISE ADCHOICES © 2016 NBCNEWS.COM

Exhibit E

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 F

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 Russian 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.

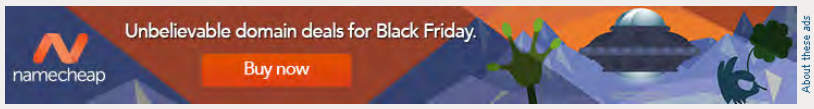
A presidential directive released in 2013 details 16 sectors that are considered critical infrastructure, including energy, financial services, healthcare, transportation, food and agriculture, and communications. The designation places responsibilities on the Homeland Security secretary to identify 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

Copyright © 2016, Chicago Tribune

This article is related to: Jeh Johnson, James Comey

Exhibit G



WORLD | PASSCODE

Share
Tweet
E-mail
More

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."

About these ads

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

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.

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

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

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.

SUBSCRIBE

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.

About these ads

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)

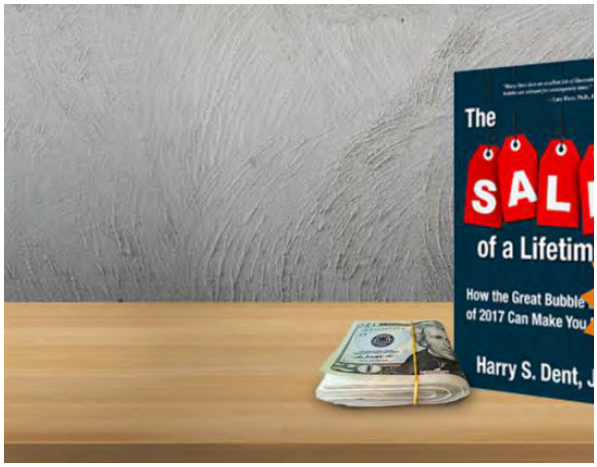
How Iran duped high-ranking US officials with fake website

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

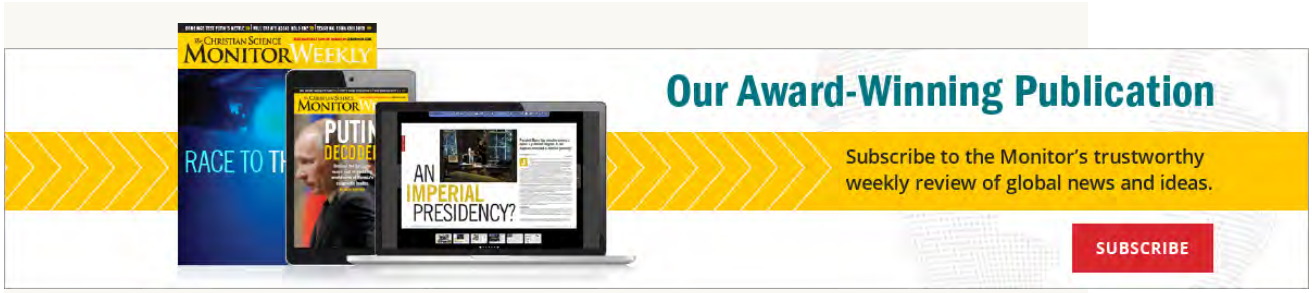
About these ads

Share Tweet E-mail More Print/Reprints

About these ads
Sponsored Content by LockerDome

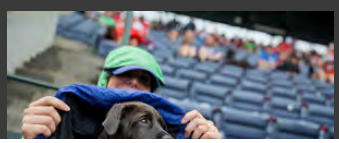


How the Great Bubble Burst of 2017 Can Make You

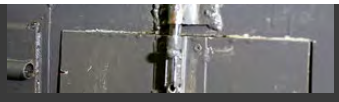


Global Galleries

Latest News

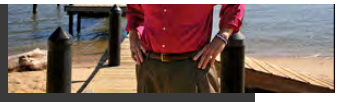


Doing Good



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

IQ Test: What is your IQ?
Answer 30 Questions to find out! View Your IQ Report Go to iq-tests-online.com
About these ads

The CHRISTIAN SCIENCE MONITOR

STAY CURRENT. GO FAR.
DISCOVER THE MONITOR DIFFERENCE

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

© The Christian Science Monitor. All Rights Reserved. Terms under which this service is provided to you. Privacy Policy.