

Gzj kdk';

AFFIDAVIT OF DAN S. WALLACH

DAN S. WALLACH, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is Dan S. Wallach. I am a Professor in the Department of Computer Science and a Rice Scholar at the Baker Institute for Public Policy at Rice University, where I have been for 18 years. My research considers a variety of topics in computer security. I also served as a member of the Air Force Science Advisory Board (2011-2015) and the USENIX Association Board of Directors (2011-2013). I've published over 100 papers in the field. I earned my M.A. (1995) and PhD (1999) from Princeton University, advised by Profs. Edward Felten and Andrew Appel. I earned my B.S. EE/CS from the University of California, at Berkeley (1993). My complete curriculum vita is attached as Exhibit A. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Michigan.
2. I've maintained a research interest in electronic voting systems starting with their widespread adoption in the early 2000s. Notably, I served as the director of an NSF-funded multi-institution research center, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), from 2005-2011. I also participated in the 2007 California "Top to Bottom Review" of its electronic voting systems, where we found unacceptable security vulnerabilities in every system we studied¹; those systems were replaced in California with more secure, paper-based systems but are still being used elsewhere and are likely still quite vulnerable. One of my ongoing projects is helping the Travis County (Austin, Texas) Clerk's office design a new electronic voting system to replace their current, aging system². In short, my experience makes me very familiar with how our election systems are vulnerable, how our adversaries might seek to exploit them, and how we can engineer better election systems for the future.
3. My main message is that our election systems face credible cyber-threats generally, and in this election year those threats are magnified in light of the persuasive evidence of state-sponsored attacks against our elections. Recounts and audits, particularly in tight races, are appropriate measures to take against these threats.

¹ <http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/>

² <https://www.usenix.org/conference/evt2013/workshop-program/presentation/bell>

Background and threat analysis

4. In September 2016, I was invited by the Congressional Space, Science, and Technology Committee to testify about possible cyber threats against our elections.³ At the time, my primary concern was attacks against voter registration databases, driven by news reports of nation-state attacks against these facilities in at least two states (Arizona and Illinois). I was and remain concerned as well about attempts to tamper with other computers systems, including those facing the voter (precinct-based optical ballot scanners and/or paperless electronic voting systems) as well as those used to do vote tabulation and reporting. I am including my Congressional testimony and post-testimony questions & answers as Exhibits B and C. My testimony speaks to the possible motives and capabilities of our nation-state adversaries toward attacking our election systems and the defenses that we have in place as well as what sort of contingency planning might be appropriate in light of these threats. I'm including some excerpts from my testimony below:
5. **How serious is the threat?** We've learned that foreign nation-state actors, likely Russian, broke into DNC computers and released documents for expressly partisan purposes⁴. So far as we know, they did this to manipulate the outcome of November's election. We must ask ourselves the same sorts of questions that arise in any security analysis. Does the adversary have the *means*, *motive*, and *opportunity* to have their desired effect, and do we have the necessary *defenses* and/or *contingency plans* to mitigate these threats?
6. **This has happened in elections before.** Russian hackers, who may or may not have been government-affiliated, committed "wanton destruction" upon Ukrainian election systems in 2014, arranging for the vote tallying system to report incorrect results⁵. The Ukrainians were lucky to catch this; it's not uncommon for nation-state computer attacks to go unnoticed for months or years. Like the Ukrainians in 2014, we face similar vulnerabilities today.

³ My written testimony:

<https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf>

My written answers to questions posed afterward:

<http://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-ga-17oct2016.pdf>

⁴ See, e.g., Lichtblau's article in the *New York Times* (July 29, 2016).

<http://www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html>

⁵ Clayton, "Ukraine election narrowly avoided wanton destruction from hackers", *Christian Science Monitor* (June 2014),

<http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video>

7. **Can our adversaries get malware into our voting machines, or our vote tabulation**

computers? The U.S. military protects its important secrets by keeping them on distinct networks and servers, physically separated from the Internet. This “air gap” defense is also used to protect voting machines. Despite this, voting machines still interact with normal computers as part of their initialization phase (loading software and ballot definitions) and the tabulation phase (extracting cast-vote records and computing the totals); these computers are not necessarily “air gapped” (see Paragraph 11, below). Even if the whole process is designed to be “air gapped” from the Internet (and it absolutely must be air-gapped), nation-state adversaries have devised a variety of workarounds. The Stuxnet malware, for example, was engineered specifically to damage nuclear centrifuges in Iran, even though those centrifuges were never connected to the Internet. We don’t know exactly how the Stuxnet malware got in, but it did nonetheless⁶.

Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems, and especially if we consider the possibility of insider threats, then yes, it’s entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries’ capabilities. The best mitigations we have for systems that we use today are only feasible where we have paper ballots. The mere *possibility* of a recount or audit of the paper ballots acts as a deterrent to an electronic attack; it’s much more difficult to tamper with paper, in bulk, relative to the effort to tamper with purely electronic records as used in many states (but not Michigan).

8. **Does an adversary need to attack everywhere?** Our adversaries understand how the American political system works. They know about “battleground states”. They can focus their efforts on states where a small nudge might have a large impact. Michigan has the smallest margin of victory in the Presidential race. This makes it a logical target.

Vote tabulation, auditing, and recounting: Validating the correct winner of the race

9. I wish to tackle a seemingly straightforward question: if there’s a risk that a nation-state attacker might have compromised some or all of the computers used in Michigan’s election systems, what steps might be appropriate to mitigate against such threats and ensure a correct election tally?
10. All votes in Michigan were marked by hand on paper, and tabulated through electronic systems. What if those electronic tabulation systems were corrupt? Manual (hand) tabulation can validate the correctness of the electronic tally, since no amount of electronic tampering can overwrite

⁶ For more details, see, e.g., Langner et al. (2013).
<http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>

paper ballots in a ballot box nor can electronic tampering compromise a team of human tabulators.

11. Why not just conduct an electronic tally? While many election officials maintain that there is “no way” their computers could have been electronically tampered, this is inconsistent with the skills available to our nation-state adversaries. For example, we know that “ballot programming” and other forms of electronic information regularly cross any “air gap” there might be around an election administrator’s computer. “Ballot programming” is the process of defining all of the candidates and races for a given election, and copying that data to the voting machines, precinct-count optical scanners, and the back-end tabulation computers. While copied around on USB sticks or other kinds of storage devices, those storage devices can also serve as a conduit for malware. (Back in the days before the Internet, PC viruses spread in exactly this fashion.)
12. It’s also a common and undesirable practice for election administrators to have their computers behind a network firewall of some sort, which is to say, there’s no actual air in the air gap. So long as there are wires between the Internet and an election administration computer, then there’s an opportunity for an adversary to break the firewall and attack the computers behind it. (Adversarial techniques to breach network firewalls are widely known to nation-state cyber attackers.)
13. Can an attacker compromise the computer inside of a precinct-based optical scanner? Unfortunately, this is well within the capabilities of a nation-state attacker. These computers are potentially vulnerable to malware that can be introduced as part of the pre-election ballot programming, wherein malware might hitch a ride along with legitimate ballot data being loaded into the scanner. There might be other vulnerabilities as well. Similar vulnerabilities were discovered as part of the California “Top to Bottom” review and the Ohio “EVEREST” studies, and we have no reason to believe that election equipment vendors have taken the engineering steps to defend against this class of attacker.
14. A purely electronic tally of paper ballots, without some sort of hand-counting or auditing would be unable to detect systematic electronic tampering--the very risk we’re concerned about in this election.
15. I have advocated and continue to support the use of “risk-limiting audits,”⁷ which have been piloted in California, Ohio, and Colorado.⁸ In short, by selecting a small number of ballots at

⁷ See, e.g., <https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf>
<http://www.commoncause.org/democracy-wire/new-post-election-audits-promise-more-accurate-election-results.html>

⁸ http://bcn.boulder.co.us/~neal/elections/corla/Risk-Limiting_Audit_Report-Final_20140331.pdf

random and then comparing the physical paper ballot with its electronic analogue, we can reach a very high degree of statistical confidence in the correctness of the election outcome. A risk-limiting audit samples a suitable number of ballots to ensure that there is no systematic error large enough to change the outcome. However, as a pragmatic matter, a risk-limiting audit is not an alternative to the full hand recount that I believe is appropriate here. Because risk-limited audits are not currently a standard practice in Michigan, their introduction would require substantial effort to agree on suitable procedures, to implement those procedures, and to train staff on those procedures to ensure the audit occurs properly. It is unlikely such procedures can be developed and implemented in the short time period at issue here.

16. Examining hand-marked paper ballots by hand is therefore the only practical approach available to mitigate against electronic corruption or tampering in the optical scanner and tabulation system.

The accuracy of a recount

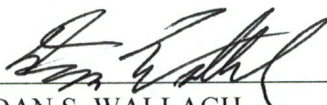
17. Even aside from the concerning issue of computer hacking, a hand recount is important to determine every vote actually cast by a voter is counted, even if the voter did not precisely mark his or her ballot. While most voters indeed follow the instructions, many don't.
18. There are many circumstances where an optical scanner will accept a ballot that might otherwise be rejected. For example, under Michigan law, if the voter signed or otherwise made personally distinguishing marks on his or her ballot, then the ballot should be properly removed from the tally,⁹ yet optical scanners will still accept it. (Ballots must be anonymous, otherwise voters will be subject to bribery or coercion.) Similarly, instead of filling in a bubble for a candidate, a voter might have written a light check mark that the machine might not pick up. Only a human vote counter can make accurate judgements on whether many ballot markings should be properly counted as votes. Other issues that might confuse a scanner include "stray marks" which a scanner sees and a human observer would clearly discount.
19. Broadly speaking, a human ballot tabulator can learn a voter's style, i.e., how they typically fill in bubbles. If most bubbles are marked in a heavy hand, it's easier to reject a light "stray mark" that a machine might otherwise count. If, on the other hand, all the bubbles are marked with light single lines, a machine might not see any of them and treat the whole ballot as if nothing were marked. A human tabulator would know that the voter used this specific style and would be able to correctly interpret the voter's intent where a machine could not.

⁹ See Mich. Elec. L. § 168.803(1)(a).

20. The correct interpretation of voter intent for individual ambiguous ballots became a point of contention in Minnesota's 2008 Senate race between Al Franken and Norm Coleman¹⁰, and similar issues might be important this year in Michigan as well.
21. *By conducting manual tallies, a recount will produce a tally that more accurately tabulates the votes cast by Michigan's voters than an electronic tally. A manual tally is particularly necessary here given the concerning evidence of Russian-sponsored hacking and the vulnerabilities of our election machinery. Luckily, Michigan is a state that has paper records of each vote which can be used to verify the election results. I believe the only appropriate recount in this circumstance is one that manually tallies those paper records.*

¹⁰ http://minnesota.publicradio.org/features/2008/11/19_challenged_ballots/

This affidavit was executed on the 30th day of November, 2016 in Houston, Texas.


DAN S. WALLACH

Sworn to before me this 30th day of November, 2016.


Notary Public

My Commission Expires: 6/04/2017

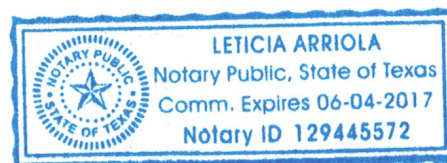


EXHIBIT A: Curriculum Vitae for Dan S. Wallach

Dan Seth Wallach

Home: 713-662-3331

Work: 713-348-6155

Fax: 713-348-5930

dwallach@cs.rice.edu<http://www.cs.rice.edu/~dwallach/>

Department of Computer Science
 Rice University
 Duncan Hall 3122
 6100 Main Street
 Houston, TX 77005

Education Princeton University (Princeton, NJ), Department of Computer Science,

Ph.D. Computer Science, January 1999.

M.A. Computer Science, May 1995.

U.C. Berkeley (Berkeley, CA), College of Engineering,

B.S. Electrical Engineering/Computer Science, May 1993.

Publications

- [1] A. Pridgen, S. Garfinkel, and D. S. Wallach. Present but unreachable: reducing persistent latent secrets in HotSpot JVM. In *Hawaii International Conference on System Sciences (HICSS-50)*, Jan. 2017. [[bib](#) | [pdf](#)]
- [2] S. Bell, J. Benaloh, M. D. Byrne, D. DeBeauvoir, B. Eakin, G. Fisher, P. Kortum, N. McBurnett, J. M. M. Parker, O. Pereira, P. B. Stark, D. S. Wallach, and M. Winn. Star-vote: A secure, transparent, auditable, and reliable voting system. In F. Hao and P. Y. A. Ryan, editors, *Real-World Electronic Voting: Design, Analysis, and Deployment*. CRC Press, Dec. 2016. [[bib](#) | [http](#)]
- [3] D. S. Wallach. Testimony before the House Committee on Space, Science & Technology hearing, protecting the 2016 elections from cyber and voting machine attacks, Sept. 2016. [[bib](#) | [pdf](#)]
- [4] Z. Tao, A. Kokas, R. Zhang, D. S. Cohan, and D. S. Wallach. Inferring atmospheric particulate matter concentrations from Chinese social media data. *PLOS One*, Sept. 2016. [[bib](#) | [http](#)]
- [5] R. S. Tanash, A. Aydogu, Z. Chen, D. S. Wallach, M. Marschall, D. Subramanian, and C. Bronk. Detecting influential users and communities in censored tweets using data-flow graphs. In *Proceedings of the 33rd Annual Meeting of the Society for Political Methodology (POLMETH 2016)*, Houston, TX, 2016. [[bib](#) | [pdf](#)]
- [6] R. S. Tanash, A. Aydogu, Z. Chen, D. S. Wallach, M. Marschall, D. Subramanian, and C. Bronk. The dynamics of social media censorship in transitioning democracies. In *The 2016 APSA Conference (Division of Political Elites and Social Media, and Information Technology and Politics)*, Philadelphia, PA, 2016. [[bib](#) | [http](#)]
- [7] J. C. Dressler, C. Bronk, and D. S. Wallach. Exploiting military opsec through open-source vulnerabilities. In *2015 IEEE Military Communications Conference (MILCOM '15)*, Tampa, FL, Oct. 2015. [[bib](#) | [pdf](#)]
- [8] R. S. Tanash, Z. Chen, T. Thakur, D. S. Wallach, and D. Subramanian. Known unknowns: An analysis of Twitter censorship in Turkey. In *Workshop on Privacy in the Electronic Society*, Denver, CO, Oct. 2015. [[bib](#)]
- [9] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach. From error to error: Why voters could not cast a ballot and verify their vote with Helios, Prêt à Voter, and Scantegrity II. *USENIX Journal of Election Technology and Systems (JETES)*, 3(2), Aug. 2015. [[bib](#) | [pdf](#)]

- [10] Y. Liu, D. R. Bild, D. Adrian, G. Singh, R. P. Dick, D. S. Wallach, and Z. M. Mao. Performance and energy consumption analysis of a delay-tolerant network for censorship-resistant communications. In *16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '15)*, June 2015. [[bib](#) | [http](#)]
- [11] D. R. Bild, Y. Liu, R. P. Dick, Z. M. Mao, and D. S. Wallach. Aggregate characterization of user behavior in Twitter and analysis of the retweet graph. *ACM Transactions on Internet Technologies*, 15(1), Feb. 2015. [[bib](#) | [http](#)]
- [12] A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security*, 23:167--195, 2015. [[bib](#) | [.pdf](#)]
- [13] Y. Liu, D. R. Bild, R. P. Dick, Z. M. Mao, and D. S. Wallach. The mason test: A defense against sybil attacks in wireless networks without trusted authorities. *IEEE Transactions on Mobile Computing*, 2015. in press. [[bib](#) | [.pdf](#)]
- [14] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach. Users' mental models for three end-to-end voting systems: Helios, Prêt à Voter, and Scantegrity II. In *Human Aspects of Information Security, Privacy, and Trust*, volume 9190 of *Lecture Notes in Computer Science*. Springer International Publishing, 2015. [[bib](#) | [DOI](#) | [http](#)]
- [15] T. Book and D. S. Wallach. An empirical study of mobile ad targeting. *CoRR*, abs/1502.06577, 2015. [[bib](#) | [http](#)]
- [16] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach. Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *USENIX Journal of Election Technology and Systems (JETS)*, 2(3), July 2014. [[bib](#) | [http](#)]
- [17] M. Dietz and D. S. Wallach. Hardening Persona: Improving federated web login. In *Network and Distributed Systems Symposium (NDSS '14)*, San Diego, CA, Feb. 2014. [[bib](#) | [.pdf](#)]
- [18] M. Rostami, M. Majzoobi, F. Koushanfar, D. S. Wallach, and S. Devadas. Robust and reverse-engineering resilient PUF authentication and key-exchange by substring matching. *IEEE Transactions on Emerging Topics in Computing*, 2014. [[bib](#) | [.pdf](#)]
- [19] A. A. Sani, L. Zhong, and D. S. Wallach. Glider: A GPU library driver for improved system security. *CoRR*, abs/1411.3777, 2014. [[bib](#) | [http](#)]
- [20] T. Book and D. S. Wallach. A case of collusion: a study of the interface between ad libraries and their apps. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM '13)*, Berlin, Germany, Nov. 2013. [[bib](#) | [.pdf](#)]
- [21] S. Bell, J. Benaloh, M. D. Byrne, D. DeBeauvoir, B. Eakin, G. Fisher, P. Kortum, N. McBurnett, J. M. M. Parker, O. Pereira, P. B. Stark, D. S. Wallach, and M. Winn. Star-vote: A secure, transparent, auditable, and reliable voting system. *USENIX Journal of Election Technology and Systems (JETS)*, 1(1), Aug. 2013. [[bib](#) | [http](#)]
- [22] T. Zhu, D. Phipps, A. Pridgen, J. Crandall, and D. S. Wallach. The velocity of censorship: High-fidelity detection of microblog post deletions. In *USENIX Security Symposium*, Washington, DC, Aug. 2013. [[bib](#) | [http](#)]
- [23] T. Book, A. Pridgen, and D. S. Wallach. Longitudinal analysis of Android ad library permissions. In *Mobile Security Technologies Workshop (MOST)*, San Francisco, CA, May 2013. [[bib](#) | [.pdf](#)]
- [24] P. Song, A. Shu, D. Phipps, D. S. Wallach, M. Tiwari, J. Crandall, and G. Lugar. Language without words: A pointillist model for natural language processing. In *6th International Conference on Soft Computing and Intelligent Systems (SCIS-ISIS 2012)*, Kobe, Japan, Dec. 2012. [[bib](#) | [.pdf](#)]
- [25] A. Czeskis, M. Dietz, T. Kohno, D. S. Wallach, and D. Balfanz. Strengthening user authentication through opportunistic cryptographic identity assertions. In *19th ACM*

Conference on Computer and Communications Security (CCS '12), Raleigh, NC, Oct. 2012. [[bib](#) | [http](#)]

- [26] P. Song, A. Shu, A. Zhou, D. S. Wallach, and J. R. Crandall. A pointillism approach for natural language processing of social media. In *Proceedings of the 2012 International Conference on Natural Language Processing and Knowledge Engineering (NLP-KE'12)*, Hefei, China, Sept. 2012. best paper award. [[bib](#) | [.pdf](#)]
- [27] M. Dietz, A. Czeskis, D. Balfanz, and D. S. Wallach. Origin-bound certificates: a fresh approach to strong client authentication for the web. In *USENIX Security Symposium*, Bellevue, WA, Aug. 2012. [[bib](#) | [http](#)]
- [28] S. Shekhar, M. Dietz, and D. S. Wallach. Adsplit: Separating smartphone advertising from applications. In *USENIX Security Symposium*, Bellevue, WA, Aug. 2012. [[bib](#) | [http](#)]
- [29] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching. In *International Workshop on Trustworthy Embedded Devices*, May 2012. [[bib](#) | [DOI](#) | [.pdf](#)]
- [30] A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. S. Wallach. Accountable wiretapping -or- I know they can hear you now. In *19th ISOC Network and Distributed System Security Symposium (NDSS 2012)*, San Diego, CA, Feb. 2012. [[bib](#) | [http](#)]
- [31] N. Aase, J. R. Crandall, A. Diaz, J. Knockel, J. O. Molinero, J. Saia, D. Wallach, and T. Zhu. Whiskey, weed, and wukan on the World Wide Web: On measuring censors' resources and motivations. In *FOCI 12: Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet*, 2012. [[bib](#) | [http](#)]
- [32] D. S. Wallach. Viewpoint: Rebooting the cs publication process. *Communications of the ACM*, 54(10), Oct. 2011. [[bib](#) | [.pdf](#)]
- [33] S. A. Crosby and D. S. Wallach. Authenticated dictionaries: Real-world costs and trade-offs. *ACM Transactions on Information Systems Security (TISSEC)*, 14(2):17:1--17:30, Sept. 2011. [[bib](#) | [DOI](#) | [http](#)]
- [34] M. Dietz, S. Shekhar, Y. Pisetsky, A. Shu, and D. S. Wallach. Quire: Lightweight provenance for smart phone operating systems. In *21st USENIX Security Symposium*, San Francisco, CA, Aug. 2011. [[bib](#) | [.html](#)]
- [35] D. R. Bild, Y. Liu, R. P. Dick, Z. M. Mao, and D. S. Wallach. Using predictable mobility patterns to support scalable and secure MANETs of handheld devices. In *Sixth International Workshop on Mobility in the Evolving Internet Architecture (MobiArch '11)*, June 2011. [[bib](#) | [http](#)]
- [36] D. S. Wallach. Smartphone security: Trends and predictions. In *Secure Application Development (SecAppDev 2011)*, Leuven, Belgium, Feb. 2011. [[bib](#) | [.pdf](#)]
- [37] T. Zhu, C. Bronk, and D. S. Wallach. An analysis of chinese search engine filtering. *CoRR*, abs/1107.3794, 2011. [[bib](#) | [http](#)]
- [38] D. Bachrach, C. Nunu, D. S. Wallach, and M. K. Wright. #h00t: Censorship resistant microblogging. *CoRR*, abs/1109.6874, 2011. [[bib](#) | [http](#)]
- [39] S. J. Nielson and D. S. Wallach. The bittorrent anonymity marketplace. *CoRR*, abs/1108.2718, 2011. [[bib](#) | [http](#)]
- [40] S. J. Nielson, C. E. Spare, and D. S. Wallach. Building better incentives for robustness in bittorrent. *CoRR*, abs/1108.2716, 2011. [[bib](#) | [http](#)]
- [41] S. A. Crosby and D. S. Wallach. High throughput asynchronous algorithms for message authentication. Technical Report CS TR10-15, Rice University, Houston, TX, Dec. 2010. [[bib](#) | [.pdf](#)]
- [42] T.-W. J. Ngan, R. Dingledine, and D. S. Wallach. Building incentives into Tor. In *Proceedings of Financial Cryptography (FC '10)*, Tenerife, Canary Islands, Jan. 2010. best paper award. [[bib](#) | [.pdf](#)]
- [43] S. A. Crosby and D. S. Wallach. *Encyclopedia of Cryptography and Security*, chapter

Algorithmic Denial of Service. Springer-Verlag, 2 edition, 2010. [[bib](#)]

- [44] D. S. Wallach. Native client: A clever alternative. *Communications of the ACM*, 53(1), Jan. 2010. [[bib](#) | [http](#)]
- [45] D. S. Wallach. Polling place burglary raises specter of fraud. *Houston Chronicle*, Dec. 2009. [[bib](#) | [http](#)]
- [46] S. A. Crosby and D. S. Wallach. Super-efficient aggregating history-independent persistent authenticated dictionaries. In *Proceedings of ESORICS 2009*, Saint Malo, France, Sept. 2009. [[bib](#) | [.pdf](#)]
- [47] S. A. Crosby and D. S. Wallach. Efficient data structures for tamper-evident logging. In *Proceedings of the 18th USENIX Security Symposium*, Montreal, Canada, Aug. 2009. [[bib](#) | [.pdf](#)]
- [48] E. Öksüzöglu and D. S. Wallach. VoteBox Nano: A smaller, stronger, FPGA-based voting machine. In *Electronic Voting Technology/Workshop on Trustworthy Elections 2009*, Montreal, Canada, Aug. 2009. [[bib](#) | [.pdf](#)]
- [49] C. Bronk, D. Castro, and D. S. Wallach. Group effort needed to secure cyberspace. *Houston Chronicle*, June 2009. [[bib](#) | [.pdf](#)]
- [50] D. R. Sandler and D. S. Wallach. Birds of a FETHR: Open, decentralized micropublishing. In *8th International Workshop on Peer-to-Peer Systems (IPTPS '09)*, Boston, MA, Apr. 2009. [[bib](#) | [.pdf](#)]
- [51] D. S. Wallach. Technical perspective: Tools for information to flow securely and swift-ly. *Communications of the ACM*, 52(2), Feb. 2009. [[bib](#) | [.pdf](#)]
- [52] S. A. Crosby, R. H. Riedi, and D. S. Wallach. Opportunities and limits of remote timing attacks. *ACM Transactions on Information and Systems Security (TISSEC)*, 12(3), Jan. 2009. [[bib](#) | [.pdf](#)]
- [53] D. S. Wallach. Voting system risk assessment via computational complexity analysis. *William and Mary Bill of Rights Journal*, 17, Dec. 2008. [[bib](#) | [.pdf](#)]
- [54] D. R. Sandler and D. S. Wallach. The case for networked remote voting precincts. In *3rd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08)*, San Jose, CA, Aug. 2008. [[bib](#) | [.pdf](#)]
- [55] D. R. Sandler, K. Derr, and D. S. Wallach. VoteBox: A tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th USENIX Security Symposium (Security '08)*, San Jose, CA, July 2008. [[bib](#) | [.pdf](#)]
- [56] D. R. Sandler and D. S. Wallach. <input type="password"> must die! In *Web 2.0 Security & Privacy (W2SP 2008)*, Oakland, CA, May 2008. [[bib](#) | [.pdf](#)]
- [57] S. Everett, K. Greene, M. Byrne, D. Wallach, K. Derr, D. Sandler, and T. Torous. Is newer always better? The usability of electronic voting machines versus traditional methods. In *Proceedings of CHI 2008*, Florence, Italy, Apr. 2008. [[bib](#) | [.html](#)]
- [58] R. M. Stein, G. Vonnahme, M. Byrne, and D. S. Wallach. Voting technology, election administration, and voter performance. *Election Law Journal*, 7(2), Apr. 2008. [[bib](#) | [.pdf](#)]
- [59] D. Sandler, K. Derr, S. Crosby, and D. S. Wallach. Finding the evidence in tamper-evident logs. In *Proceedings of the 2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '08)*, pages 69--75, 2008. [[bib](#) | [DOI](#) | [http](#)]
- [60] D. R. Sandler and D. S. Wallach. Casting votes in the Auditorium. In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, Boston, MA, Aug. 2007. [[bib](#) | [.pdf](#)]
- [61] S. Inguva, E. Rescorla, H. Shacham, and D. S. Wallach. *Source Code Review of the Hart InterCivic Voting System*. California Secretary of State's "Top to Bottom" Review, July 2007. [[bib](#) | [.pdf](#)]

- [62] D. L. Dill and D. S. Wallach. *Stones Unturned: Gaps in the Investigation of Sarasota's Disputed Congressional Election*, Apr. 2007. [[bib](#) | [html](#)]
- [63] D. S. Wallach. Security and Reliability of Webb County's ES&S Voting System and the March '06 Primary Election. Expert Report in *Flores v. Lopez*, May 2006. [[bib](#) | [pdf](#)]
- [64] A. Singh, T.-W. J. Ngan, P. Druschel, and D. S. Wallach. Eclipse attacks on overlay networks: Threats and defenses. In *IEEE INFOCOM '06*, Barcelona, Spain, Apr. 2006. [[bib](#) | [pdf](#)]
- [65] C. Coarfa, P. Druschel, and D. S. Wallach. Performance analysis of tls web servers. *ACM Transactions on Computer Systems*, 24(1), Feb. 2006. [[bib](#) | [pdf](#)]
- [66] A. Nandi, T.-W. J. Ngan, A. Singh, P. Druschel, and D. S. Wallach. Scrivener: Providing incentives in cooperative content distribution systems,. In *ACM/IFIP/USENIX 6th International Middleware Conference (Middleware 2005)*, Grenoble, France, Nov. 2005. [[bib](#) | [html](#)]
- [67] E. de Lara, Y. Chopra, R. Kumar, N. Vaghela, D. S. Wallach, and W. Zwaenepoel. Iterative adaptation for mobile clients using existing APIs. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 16(10), Oct. 2005. [[bib](#) | [html](#)]
- [68] S. J. Nielson, S. A. Crosby, and D. S. Wallach. A taxonomy of rational attacks. In *4th International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, NY, Feb. 2005. [[bib](#) | [html](#)]
- [69] A. B. Stubblefield, A. D. Rubin, and D. S. Wallach. Managing the performance impact of web security. *Electronic Commerce Research Journal*, 5(1), Feb. 2005. [[bib](#) | [pdf](#)]
- [70] A. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, and D. S. Wallach. Robotics-based location sensing using wireless Ethernet. *Wireless Networks*, 11(1-2), Jan. 2005. [[bib](#) | [http](#)]
- [71] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudys, D. S. Wallach, and L. E. Kavraki. Practical robust localization over large-scale wireless Ethernet networks. In *Tenth ACM International Conference on Mobile Computing and Networking (MOBICOM 2004)*, Philadelphia, PA, Sept. 2004. [[bib](#) | [pdf](#)]
- [72] A. Mislove, G. Oberoi, A. Post, C. Reis, P. Druschel, and D. S. Wallach. AP3: Cooperative, decentralized anonymous communication. In *11th ACM SIGOPS European Workshop*, Leuven, Belgium, Sept. 2004. [[bib](#) | [html](#)]
- [73] D. S. Wallach. Texas must confront voting systems' flaws. *Austin American-Statesman*, Sept. 2004. [[bib](#) | [pdf](#)]
- [74] T.-W. J. Ngan, A. Nandi, A. Singh, D. S. Wallach, and P. Druschel. Designing incentives-compatible peer-to-peer systems. In *2nd Bertinoro Workshop on Future Directions in Distributed Computing (FuDiCo 2004)*, Bertinoro, Italy, June 2004. [[bib](#) | [html](#)]
- [75] A. M. Ladd, K. E. Bekris, A. Rudys, D. S. Wallach, and L. E. Kavraki. On the feasibility of using wireless Ethernet for localization. *IEEE Transactions on Robotics and Automation*, 20(3):555--559, June 2004. [[bib](#) | [pdf](#)]
- [76] T.-W. J. Ngan, D. S. Wallach, and P. Druschel. Incentives-compatible peer-to-peer multicast. In *2nd Workshop on Economics of Peer-to-Peer Systems*, Cambridge, MA, June 2004. [[bib](#) | [html](#)]
- [77] D. S. Wallach. Testimony for the Texas Senate Committee on State Affairs, May 2004. [[bib](#) | [pdf](#)]
- [78] D. S. Wallach. Testimony for the Texas House Committee on Elections, Mar. 2004. [[bib](#) | [pdf](#)]
- [79] D. S. Wallach. Testimony for the Ohio Joint Committee on Ballot Security, Mar. 2004. [[bib](#) | [pdf](#)]
- [80] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*,

Oakland, CA, 2004. [[bib](#) | [http](#)]

- [81] J. Bannet, D. W. Price, A. Rudys, J. Singer, and D. S. Wallach. Hack-a-Vote: Demonstrating security issues with electronic voting systems. *IEEE Security and Privacy Magazine*, 2(1):32--37, January / February 2004. Also reprinted by ComputerUser, March 2004. [[bib](#) | [.pdf](#)]
- [82] P. Tao, A. Rudys, A. Ladd, and D. S. Wallach. Wireless LAN location sensing for security applications. In *ACM Workshop on Wireless Security (WiSe 2003)*, San Diego, CA, Sept. 2003. [[bib](#) | [.html](#)]
- [83] S. Crosby and D. S. Wallach. Denial of service via algorithmic complexity attacks. In *12th Usenix Security Symposium*, Washington, D.C., Aug. 2003. [[bib](#) | [.pdf](#)]
- [84] A. C. Fuqua, T.-W. J. Ngan, and D. S. Wallach. Economic behavior of peer-to-peer storage networks. In *Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, June 2003. [[bib](#) | [.html](#)]
- [85] D. W. Price, A. Rudys, and D. S. Wallach. Garbage collector memory accounting in language-based systems. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003. [[bib](#) | [.html](#)]
- [86] A. Mislove, A. Post, C. Reis, P. Willmann, P. Druschel, D. S. Wallach, X. Bonnaire, P. Sens, J.-M. Busca, and L. Arantes-Bezerra. POST: A secure, resilient, cooperative messaging system. In *9th Workshop on Hot Topics in Operating Systems (HotOS IX)*, Lihue, Hawaii, May 2003. [[bib](#) | [.html](#)]
- [87] E. de Lara, R. Kumar, D. S. Wallach, and W. Zwaenepoel. Collaboration and multimedia authoring on mobile devices. In *First International Conference on Mobile Systems, Applications, and Services (MobiSys '03)*, San Francisco, CA, May 2003. [[bib](#) | [.pdf](#)]
- [88] N. Paul, D. Evans, A. D. Rubin, and D. S. Wallach. Authentication for remote voting. In *Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, FL, Apr. 2003. [[bib](#) | [.html](#)]
- [89] T.-W. J. Ngan, D. S. Wallach, and P. Druschel. Enforcing fair sharing of peer-to-peer resources. In *Proceedings of the Second International Workshop on Peer-to-Peer Systems*, Berkeley, CA, Feb. 2003. [[bib](#) | [.html](#)]
- [90] Y. C. Hu, W. Yu, A. L. Cox, D. S. Wallach, and W. Zwaenepoel. Runtime support for distributed sharing in safe languages. *ACM Transactions on Computer Systems*, 21(1), 2003. [[bib](#) | [.pdf](#)]
- [91] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach. Security for structured peer-to-peer overlay networks. In *Fifth Symposium on Operating Systems Design and Implementation (OSDI '02)*, Boston, MA, Dec. 2002. [[bib](#) | [.html](#)]
- [92] A. Rudys and D. S. Wallach. Enforcing Java run-time properties using bytecode rewriting. In *International Symposium on Software Security*, Tokyo, Japan, Nov. 2002. [[bib](#) | [.html](#)]
- [93] D. S. Wallach. A survey of peer-to-peer security issues. In *International Symposium on Software Security*, Tokyo, Japan, Nov. 2002. [[bib](#) | [.html](#)]
- [94] A. M. Ladd, K. E. Bekris, G. Marceau, A. Rudys, D. S. Wallach, and L. E. Kavraki. Using wireless Ethernet for localization. In *2002 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2002)*, Lausanne, Switzerland, Oct. 2002. [[bib](#) | [.pdf](#)]
- [95] A. M. Ladd, K. E. Bekris, G. Marceau, A. Rudys, L. E. Kavraki, and D. S. Wallach. Robotics-based location sensing using wireless Ethernet. In *Eighth ACM International Conference on Mobile Computing and Networking (MOBICOM 2002)*, Atlanta, Georgia, Sept. 2002. [[bib](#) | [.pdf](#)]
- [96] Y. Dotsenko, E. de Lara, D. S. Wallach, and W. Zwaenepoel. Extensible adaptation via constraint solving. In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, June 2002. [[bib](#) | [http](#)]

- [97] A. Rudys and D. S. Wallach. Transactional rollback for language-based systems. In *2002 International Conference on Dependable Systems and Networks*, Washington, D.C., June 2002. [[bib](#) | [html](#)]
- [98] A. Rudys and D. S. Wallach. Termination in language-based systems. *ACM Transactions on Information and System Security*, 5(2), May 2002. [[bib](#) | [html](#)]
- [99] C. Coarfa, P. Druschel, and D. S. Wallach. Performance analysis of TLS Web servers. In *Proceedings of the 2002 Network and Distributed System Security Symposium*, San Diego, CA, Feb. 2002. [[bib](#) | [html](#)]
- [100] E. de Lara, D. S. Wallach, and W. Zwaenepoel. HATS: Hierarchical adaptive transmission scheduling. In *Proceedings of the 2002 Multimedia Computing and Networking Conference (MMCN'02)*, San Jose, CA, Jan. 2002. [[bib](#) | [http](#)]
- [101] J. Flinn, E. de Lara, M. Satyanarayanan, D. S. Wallach, and W. Zwaenepoel. Reducing the energy usage of Office applications. In *Proceedings of IFIP/ACM International Conference on Distributed Systems Platforms (Middleware)*, Heidelberg, Germany, Nov. 2001. [[bib](#) | [http](#)]
- [102] D. S. Wallach. Copy protection technology is doomed. *IEEE Computer*, 34(10):48--49, Oct. 2001. [[bib](#) | [pdf](#)]
- [103] S. A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. S. Wallach, D. Dean, and E. W. Felten. Reading between the lines: Lessons from the SDMI challenge. In *10th Usenix Security Symposium*, Washington, D.C., Aug. 2001. [[bib](#) | [pdf](#)]
- [104] A. Stubblefield and D. S. Wallach. Dagster: Censorship-resistant publishing without replication. Technical Report TR01-380, Rice University, July 2001. [[bib](#) | [pdf](#)]
- [105] E. de Lara, D. S. Wallach, and W. Zwaenepoel. Puppeteer: Component-based adaptation for mobile computing. In *Proceedings of the 3rd USENIX Symposium on Internet Technologies and Systems (USITS)*, San Francisco, CA, Mar. 2001. [[bib](#) | [http](#)]
- [106] A. Rudys, J. Clements, and D. S. Wallach. Termination in language-based systems. In *Network and Distributed Systems Security Symposium*, San Diego, CA, Feb. 2001. [[bib](#) | [html](#)]
- [107] D. S. Wallach, E. W. Felten, and A. W. Appel. The security architecture formerly known as stack inspection: A security mechanism for language-based systems. *ACM Transactions on Software Engineering and Methodology*, 9(4):341--378, Oct. 2000. [[bib](#) | [html](#)]
- [108] E. de Lara, D. S. Wallach, and W. Zwaenepoel. Opportunities for bandwidth adaptation in Microsoft Office documents. In *Proceedings of the Fourth USENIX Windows Symposium*, Seattle, Washington, Aug. 2000. [[bib](#) | [http](#)]
- [109] A. Grosul and D. S. Wallach. A related-key cryptanalysis of RC4. Technical Report TR-00-358, Department of Computer Science, Rice University, Houston, TX, June 2000. [[bib](#) | [pdf](#)]
- [110] A. B. Stubblefield and D. S. Wallach. A security analysis of My.MP3.com and the Beam-it protocol. Technical Report TR-00-353, Department of Computer Science, Rice University, Houston, TX, Feb. 2000. [[bib](#) | [html](#)]
- [111] D. S. Wallach. *A New Approach to Mobile Code Security*. PhD thesis, Princeton University, Princeton, NJ, Jan. 1999. [[bib](#) | [html](#)]
- [112] D. S. Wallach and E. W. Felten. Understanding Java stack inspection. In *Proceedings of the 1998 IEEE Symposium on Security and Privacy*, pages 52--63, Oakland, CA, May 1998. [[bib](#) | [html](#)]
- [113] E. W. Felten, D. Balfanz, D. Dean, and D. S. Wallach. Web spoofing: An Internet con game. In *20th National Information Systems Security Conference*, Baltimore, Maryland, Oct. 1997. [[bib](#) | [html](#)]
- [114] D. Dean, E. W. Felten, D. S. Wallach, and D. Balfanz. Java security: Web browsers and

- beyond. In D. E. Denning and P. J. Denning, editors, *Internet Besieged: Countering Cyberspace Scofflaws*, pages 241--269. ACM Press, New York, NY, Oct. 1997. [[bib](#) | [html](#)]
- [115] D. S. Wallach, D. Balfanz, D. Dean, and E. W. Felten. Extensible security architectures for Java. In *Proceedings of the Sixteenth ACM Symposium on Operating System Principles*, Saint-Malo, France, Oct. 1997. outstanding paper award. [[bib](#) | [html](#)]
- [116] D. S. Wallach, J. A. Roskind, and E. W. Felten. Flexible, extensible Java security using digital signatures. In *DIMACS Workshop on Network Threats*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, Dec. 1996. [[bib](#)]
- [117] D. Dean, E. W. Felten, and D. S. Wallach. Java security: From HotJava to Netscape and beyond. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pages 190-200, Oakland, CA, May 1996. [[bib](#) | [html](#)]
- [118] D. S. Wallach, S. Kunapalli, and M. F. Cohen. Accelerated MPEG compression of dynamic polygonal scenes. In *Computer Graphics (Proceedings of SIGGRAPH 1994)*, Orlando, FL, July 1994. [[bib](#) | [http](#)]

Teaching

Courses at Rice:

- Comp215: [Introduction to Program Design](#) (Fall 2014-2016)
- Comp327 / 427: [Introduction to Computer Security](#) (Spring 2011-2017)
- Comp527: [Computer Systems Security](#) (Spring 1999, Fall and Spring 2000, Fall 2001-2006, 2008-2013)
- Comp435: [Election Systems, Technology, and Administration](#) (Fall 2006, Fall 2008, Fall 2012, Fall 2016)
- Comp314: [Applied Algorithms and Data Structures](#) (Fall 1999, Spring 2001, 2002, 2004-2006, 2008-2010)
- Comp620: [Seminar in Secure Systems](#) (Fall 1998)

Short courses and tutorials:

- Dan S. Wallach, *SecVote Summer School* (Schloss Dagstuhl, Germany), July 2012.
- Dan S. Wallach, *Software Engineering for Security* (a one-week intensive short course), presented at [Secure Application Development](#) (Leuven, Belgium), February 2016, (also February 2011 and February 2007).
- Dan S. Wallach, *Software Engineering for Security* (lectures), presented at [4th International School: Network Security Impact on Quality Software Engineering](#) (Viña del Mar & Valparaíso, Chile), October 2007.
- Dan S. Wallach, *Language-Based Security* (a one-week intensive short course), presented at *The ACM Summer School on Foundations of Internet Security* (Duszniki Zdrój, Poland), June 2002.
- Dan S. Wallach and Drew Dean, *Java and Security* (a one-week intensive short course), [Katholieke Universiteit Leuven](#) (Leuven, Belgium), March 1997.

Teaching assistant positions at Princeton:

- [Introduction to Computer Systems](#) (Spring 1996)
- [Computer Graphics](#) (Fall 1993, Fall 1994, and Fall 1995)
- [Advanced Programming Techniques](#) (Spring 1994)

Professional Service *Research management:*

Associate Director, ACCURATE (NSF-funded research center), 2005-2010
Acting Director (ACCURATE), 2010-2011

National service / advisory boards:

[Air Force Science Advisory Board](#) (2011-2015)
[USENIX Association](#), Board of Directors (2012-2013)
USENIX Security, Steering Committee (2014-present)

Program committees:

ACM Conference on Computer and Communications Security (CCS) 2004, 2005, 2008, 2009
ACM Conference on Electronic Commerce 2007
ACM Role-Based Access Control Workshop 1999 and 2000
ACM SIGPLAN Third Workshop on Programming Languages and Analysis for Security (PLAS) 2008
Applied Cryptography and Network Security (ACNS) 2005
Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH) 2008
European Symposium on Research in Computer Security (ESORICS) 2009
Google Native Client (NaCl) Security Contest 2009
HotOS Workshop 2003, 2009, 2011
HotSec Workshop 2006
IEEE International Conference on Distributed Computing Systems (ICDCS) 2007
IEEE Security and Privacy 1999, 2004, 2005, 2007-2012
IEEE Workshop on Mobile Computing Systems and Applications (WMCSA) 2002 and 2004
3rd International Conference on Electronic Voting 2008
International Peer-to-Peer Symposium (IPTPS) 2004 and 2006
International Symposium on Engineering Secure Software and Systems (ESSoS) 2010
Network and Distributed Systems Security Symposium (NDSS) 2002-2004, 2006, and 2012
NSF grant panels 2002, 2004, 2005, 2006, 2007, 2010, 2013
South Central Information Security Symposium (SCISS) 2003-2006
USENIX Electronic Voting Technology Workshop/Workshop on Technology for Elections (EVT/WOTE) 2006-2010
USENIX Annual Technical Conference 2001
USENIX Security Symposium 1999-2003, 2005, 2011, 2012, 2014
USENIX Symposium on Internet Technologies and Systems (USITS) 2003
VOTE-ID 2009
Workshop on Economics in Peer-to-Peer Systems 2004
Workshop on Secure Execution of Untrusted Code (SecuCode) 2009
Workshop on Technology for Elections (WOTE) 2008
Workshop on Web 2.0 Security & Privacy (W2SP) 2007-2010
WWW Conference 1999, 2000, 2003, 2004, 2006-2008, 2011, 2014

Program committee chair / journal editorship:

[International Symposium on Engineering Secure Software and Systems \(ESSoS\) 2010](#)
[USENIX Security Symposium 2001](#)
[USENIX Journal of Election Technology and Systems \(JETS\)](#) (2013-2015)
[WWW Conference](#), Co-Chair of Security, Privacy, Reliability, and Ethics Track 2007 and 2008

Invited talks committee:

[USENIX Security Symposium 2002](#) and 2011

Panel moderator/organizer (electronic voting security):

[USENIX Security Symposium 2003](#)

IEEE Symposium on Security and Privacy 2004

Workshop organizer / co-chair:

[International Symposium on Engineering Secure Software and Systems \(ESSoS\) 2010](#)

South Central Information Security Symposium (SCISS) 2003-2006

[USENIX/ACCURATE Electronic Voting Technology Workshop \(EVT\) 2006](#)

Workshop on Web 2.0 Security & Privacy (W2SP) 2007-2011

Editorial and advisory board memberships:

Election Assistance Commission - Voting System Risk Analysis (EAC VSRA) panel (2008-2009)

[Election Science Institute \(VoteWatch\)](#)

[IEEE Internet Computing](#) (2004-2006)

[International Journal of Information Security](#)

[International Journal of Information and Computer Security](#)

[International Journal for Infonomics](#)

[National Committee for Voting Integrity](#)

[SAFECode](#)

[Verified Voting Foundation / VerifiedVoting.org](#)

University committees:

Advisor for MCS Students (2000-2001)

CS Graduate Admissions (1998-2005, 2014-present)

CS Curriculum Committee (2005-present)

CS Facilities (occasional involvement)

KTRU (Rice Radio) Friendly Committee (2005-dissolution of committee)

Rice Childcare Advisory Committee (2005-2006)

University IT Security Committee (2002-dissolution of committee)

Distinguished Alumni Award Selection Committee (2009)

University Benefits Committee (2011-present)

Other university service:

Divisional advisor and faculty associate, Martel College (2001-present)

Rice Social Dance Society: faculty sponsor, instructor, workshop organizer, etc. (2001-present)

External university service:

University of Cyprus, CS faculty search, external committee member (2015)

Honors and Awards

2013 Microsoft SEIF Faculty Research Award

2012 Best Paper Award (*Natural Language Processing and Knowledge Engineering*)

2011 National Centers of Academic Excellence in Information Assurance Research (CAE-R)

2010 Best Paper Award (*Financial Cryptography*)

2009 Google Research Award

2008 Kavli Frontiers of Science Fellow

2008 VoteRescue "Champion of Election Integrity" Award

2008 [Defense Science Study Group](#) (DSSG), class of 2008-2009

2007 ComputerWorld "40 Under 40" Award

2000 NSF CAREER Award

2000 IBM University Partnership Award

1997 Outstanding Paper Award (*Symposium on Operating Systems Principles*)

Related student awards

2011 National Physical Sciences Consortium (NPSC) Fellowship - Adam Pridgen

2009 Usenix Security Grand Challenge (Capture the Flag) Contest - Mike Dietz

2002 CRA Outstanding Undergraduate Award - Adam Stubblefield

Grants

Dan S. Wallach and Phil Kortum, TWC: TTP Option: Medium: Voting Systems Architectures for Security and Usability, NSF CNS-1409401 (March 2014).

Dan S. Wallach and Jedidiah R. Crandall, TWC: Medium: Collaborative: Measurement and Analysis Techniques for Internet Freedom on IP and Social Networks, NSF CNS-1314492 (July 2013).

Dan S. Wallach, TC: Small: Security Architectures for Smartphones, NSF CNS-1117943 (July 2011).

Robert Dick, Z. Morley Mao, and Dan S. Wallach, TC: Medium: Collaborative Research: WHISPER - Wireless Handheld Infrastructureless, Secure Communications System for the Prevention of Eavesdropping and Reprisal, NSF CNS-0964566 (February 2010).

Aviel D. Rubin, Dan S. Wallach, Michael Byrne, Douglas W. Jones, David Dill, Dan Boneh, David A. Wagner, Dierdre Mulligan, Drew Dean, and Peter G. Neumann, CT-CS: A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE), NSF CNS-0524211 (October 2005).

Dan S. Wallach and Peter Druschel, CSR/PDOS: Security and Incentives for Overlay Network Infrastructure, NSF CNS-0509297 (August 2005).

Dan S. Wallach and Mike Dahlin, Resource Management for Safe Deployment of Edge Services, Texas Advanced Technology Program #003604-0053-2001 (October 2001).

Dan S. Wallach, Security and Resource Management in Type-Safe Language Environments, NSF CAREER CCR-9985332 (March 2000).

Behnaam Aazhang, Richard G. Baraniuk, Joseph R. Cavallaro, Edward W. Knightly, and Dan S. Wallach, Seamless Multitier Wireless Networks for Multimedia Applications, NSF Special Projects ANI-9979465 (April 1999).

Industrial gifts and support:

Samsung research contract (September 2012)

Houston Infraguard (September 2010)

Google gift (November 2009)

Microsoft gift (November 2002)

Schlumberger gift (February 2002)

IBM University Partnership Program (June 2000)

Microsoft gift (July 2000)

Related support:

**Invited
Talks and
Panels**

1. Dan S. Wallach, *STAR-Vote: A Secure, Transaprent, Auditable, and Reliable Voting System*. SUMIT (University of Michigan, Ann Arbor, MI), October 2016.
2. Dan S. Wallach, *STAR-Vote: A Secure, Transaprent, Auditable, and Reliable Voting System*. Two Sigma (Houston, TX), October 2016.
3. Dan S. Wallach, *Internet Application Censorship: Studies of Weibo in China and Twitter in Turkey*, Houston Kiwanis (Houston, TX), July 2016.
4. Dan S. Wallach, *Internet Application Censorship: Studies of Weibo in China and Twitter in Turkey*, Stanford University (Stanford, CA), June 2016.
5. Dan S. Wallach, *Internet Application Censorship: Studies of Weibo in China and Twitter in Turkey*, OWASP Meeting, K.U. Leuven (Leuven, Belgium), February 2016.
6. Dan S. Wallach, *Security Architectures for Smartphones*, University of Texas, at Dallas (Dallas, TX), October 2015.
7. Dan S. Wallach, *Tracking, Privacy, and Network Neutrality*, Houston Kiwanis (Houston, TX), September 2015.
8. Harley Geiger, Andrew Napolitano, David Leebron, and Dan S. Wallach, *Privacy in the Digital Age*, Baker Institute for Public Policy, Rice University (Houston, TX), April 2015.
9. Dan S. Wallach, *Android WebView security and the mobile advertising marketplace*, Google Security Summit (Mountain View, CA), March 2015..
10. Dan S. Wallach, *Rice Tizen Analysis for Security*, Tizen Developers Conference (San Francisco, CA), June 2014.
11. Dan S. Wallach, *STAR-Vote: A Secure, Transaprent, Auditable, and Reliable Voting System*. National Science Foundation (Arlington, VA), May 2014.
12. Dan S. Wallach, *STAR-Vote: A Secure, Transaprent, Auditable, and Reliable Voting System*. Electronic Voting Network Conference (San Diego, CA), March 2014.
13. Dan S. Wallach, *Security Architectures for Smartphones*, Korea Advanced Institute for Science and Technology (KAIST) (Daejeon, South Korea), August 2013.
14. Dan S. Wallach, *Security Analysis of LLVM Bitcode Files for Mobile Platforms*, Tizen Developers Conference (San Francisco, CA), May 2013.
15. Dan S. Wallach, *STAR-Vote: A Secure, Transaprent, Auditable, and Reliable Voting System*. Mid-Atlantic Collegiate Cyber Defense Competition (Laurel, MD), April 2013.
16. Dan S. Wallach, *STAR-Vote: A Secure, Transaprent, Auditable, and Reliable Voting System*. Verifiable Voting Schemes Workshop (Luxembourg), March 2013. Dan S. Wallach, [*Privacy and Tracking on the Internet*](#), FTC Workshop on The Big Picture: Comprehensive Data Collection (Washington, D.C.), December 2012.
17. Dan S. Wallach, David Wagner, Philip B. Stark, and Philip Kortum. *The Future of E-Voting - Remote, Internet-Based, and Secure?* E-Voting: Risk and Opportunity (Center for Information Technology Policy at Princeton University - [Webcast Seminar](#)), November 2012.
18. Dan S. Wallach, *Security Architectures for Smartphones*, University of Luxembourg, November 2012.
19. Dan S. Wallach, *The USENIX Association: A Financial Case Study for Open Access*. Perspectives Workshop: Publication Culture in Computing Research (Schloss Dagstuhl, Germany), November 2012.

20. Dan S. Wallach, *Security Architectures for Smartphones*, National Security Agency (Ft. Meade, Maryland), June 2012.
21. Dana DeBeauvoir, Dan S. Wallach, et al. *Future of Voting Systems*, International Association of Clerks, Records, Election Officials, and Treasurers, Annual Conference (Albuquerque, New Mexico), June 2012.
22. Dan S. Wallach, *Security Architectures for Smartphones*, University of California, at Berkeley (Berkeley, California), May 2012.
23. Jonathan Blow, Adam Glass, Piau Na, and Dan S. Wallach. *CS Alumni Panel*, University of California, at Berkeley (Berkeley, California), May 2012.
24. Dan S. Wallach, *Security Architectures for Smartphones*, University of New Mexico (Albuquerque, New Mexico), April 2012.
25. Dan S. Wallach, *Thoughts on Travis County's Next-Generation Voting System*, Travis County Election Study Group (Austin, Texas), October 2011.
26. Pamela Smith, Dan S. Wallach, Ian S. Piper, and Carolyn Crnich, *Panel: The Present, Election Integrity: Past, Present, and Future - Caltech/MIT Voting Technology Project* (Cambridge, Massachusetts), October 2011.
27. Dan S. Wallach, *Quire: Lightweight Provenance for Smart Phone Operating Systems*, Technischen Universität Darmstadt (Darmstadt, Germany), July 2011.
28. Dan S. Wallach, *VoteBox: A Verifiable, Tamper-Evident, Electronic Voting System*, Distinguished Lecture, Université du Luxembourg, July 2011.
29. Dan S. Wallach, *Crypto and e-Voting: Homomorphisms, Zero-Knowledge Proofs, and Other Tricks of the Trade*, Leuven Center on Information Communication and Technology (LICT) Distinguished Lecture (Leuven, Belgium), March 2011.
30. Dan S. Wallach, *Seguridad Informática, Tendencias y Aplicaciones (Information Security Trends and Applications)*, Technology, Connectivity and Internet Workshop, Consejo Federal de Inversiones (Buenos Aires, Argentina), February 2011.
31. Dan S. Wallach, *Electronic Voting Systems: Failures and Research Opportunities*, Rice University - Scienica Lecture Series (Houston, Texas), October 2010.
32. Ann Harris Bennett, Don Cook, Stan Stanart, *Harris County Clerk Debate*, sponsored by the Houston League of Women Voters and Rice University, moderated by Dan S. Wallach, October 2010.
33. Dan S. Wallach, [The Word](#), *4th Electronic Voting Technology Workshop / Workshop on Trusted Elections (EVT/WOTE '10)* (Washington, D.C.), August 2010.
34. Dan S. Wallach, *Adventures in Electronic Voting Research*, Texas A&M University (College Station, Texas), October 2009.
35. Dan S. Wallach, *Adventures in Electronic Voting Research*, Swiss Federal Institute of Technology (ETH) (Zürich, Switzerland), May 2009.
36. Jeremy Epstein, Douglas W. Jones, E. John Sebes, David Wagner, Dan Wallach, *Electronic Voting Panel*, RSA Conference (San Francisco, California), May 2009.
37. Dan S. Wallach, *Adventures in Electronic Voting Research*, Bay Area Association of Democratic Women (Clear Lake, Texas), April 2009.
38. Dan S. Wallach, *Testimony Before the Colorado Election Reform Commission* (Denver, Colorado), December 2008.
39. Dan S. Wallach, *Adventures in Electronic Voting Research*, National Academy of Science - Kavli Frontiers of Science Symposium (Irvine, California), November 2008.
40. Dan S. Wallach, *Adventures in Electronic Voting Research*, Duke University, October 2008.

41. Dan S. Wallach, [Testimony Before the Texas Senate Committee on State Affairs](#) (Austin, Texas), October 2008.
42. Dan S. Wallach et al., *Experts Meeting – E-voting in the 2008 U.S. Elections*. The Carter Center (Atlanta, Georgia), September 2008.
43. David Beirne, Doug Chapin, Dana DeBeauvoir, Anne McGeehan, Rosemary Rodriguez, Dan S. Wallach. *Voting System Integrity: Can We Be Confident in the Accuracy of the Results?* LBJ School of Public Affairs, UT Austin (Austin, Texas), September 2008.
44. Chandler Davidson, Bob Stein, Dan S. Wallach, Tova Wang. *Democracy, Disenfranchisement, and November 2008 (Constitution Day Panel)*. Rice University (Houston, Texas), September 2008.
45. Dan S. Wallach, [Testimony Before the Texas House Committee on Elections](#) (Austin, Texas), June 2008.
46. Dan S. Wallach, *Adventures in Electronic Voting Research*, Invited Talk, West University Democrats, April 2008.
47. Dan S. Wallach, *Adventures in Electronic Voting Research*, Invited Talk, *How We Vote Conference*, Institute of the Bill of Rights, College of William & Mary (Williamsburg, Virginia), March 2008.
48. Dan S. Wallach, *Adventures in Electronic Voting Research*, Invited Talk, *Hanzen-Martel Lecture Series*, Rice University (Houston, Texas), February 2008.
49. Dan S. Wallach, *Adventures in Electronic Voting Research*, Invited Talk, *Alumni College Weekend*, Rice University (Houston, Texas), February 2008.
50. Dan S. Wallach, [Adventures in Electronic Voting Research](#), Invited Talk, Google (Mountain View, California), December 2007.
51. Dan S. Wallach, *Real-world Electronic Voting*, National Lawyers Council: National Leadership Convention (Washington, D.C.), November 2007.
52. Dan S. Wallach, *Real-world Electronic Voting*, Claim Democracy Conference (Washington, D.C.), November 2007.
53. Dan S. Wallach, [Testimony Before the Tennessee Advisory Commission on Intergovernmental Relations](#) (Nashville, Tennessee), September 2007.
54. Dan S. Wallach and J. Alex Halderman, *Results from the California Top-to-Bottom Voting Systems Review*, Presentation at Schloss Dagstuhl's [Frontiers of Electronic Voting](#) (Wadern, Germany), August 2007.
55. Michael E. Clark, Joseph E. Savage, Peter Toren, and Dan S. Wallach, *Trade Secret and Confidential Information*, Panel at the ABA National Institute on Computing and the Law (San Francisco, California), June 2007.
56. Dan S. Wallach, [Testimony Before the Senate Committee on Rules and Administration, Hearing on Electronic Election Reform](#) (Washington, D.C.), February 2007.
57. Dan S. Wallach, *Electronic Voting: Risks and Research*, Institute for Security Technology Studies Distinguished Speaker Series, Dartmouth College (Hannover, New Hampshire), October 2006.
58. Dan S. Wallach, *Electronic Voting: Risks and Research*, Max Planck Institute for Software Systems (Saarbrücken, Germany), October 2006.
59. Dan S. Wallach, *Electronic Voting: Risks and Research*, , Chaire Internationale en Sécurité Informatique, Institut Eurécom (Sophia Antipolis, France), October 2006.
60. Dan S. Wallach, *Electronic Voting: Risks and Research*, University of Texas at Austin (Austin, TX), September 2006.

61. Dan S. Wallach, *The Risks of Electronic Voting*, Election Protection Summit (Washington, D.C.), June 2006.
62. Dan S. Wallach, *Computer Security Education at Rice*, Workshop on Information Assurance Education (Houston, Texas), May 2006.
63. Dan S. Wallach, *The Risks of Electronic Voting*, Georgia Institute of Technology (Atlanta, Georgia), March 2006.
64. Dan S. Wallach, Testimony for the California Senate Elections, Reapportionment & Constitutional Amendments Committee (Menlo Park, California), February 2006.
65. Elizabeth Hanshaw Winn and Dan S Wallach, *Panel: Electronic Voting Technology*, First Annual Legislative and Public Policy Conference, TSU Thurgood Marshall School of Law (Houston, Texas), October 2005.
66. Paul Craft, Douglas Jones, John Kelsey, Ronald Rivest, Michael Shamos, Dan Tokaji, Dan S. Wallach, *Panel: Threat Discussion on Trojan Horses, Backdoors, and Other Voting System Software-Related Problems*, NIST Workshop on Threats to Voting Systems (Gaithersburg, Maryland), October 2005.
67. Dan S. Wallach, *The Risks of Electronic Voting*, Virginia Joint Committee Studying Voting Equipment (Richmond, Virginia), August 2005.
68. Dan S. Wallach, *The Risks of Electronic Voting*, Tarrant County Democratic Party Meeting (Hurst, Texas), July 2005.
69. Dan S. Wallach, *Electronic Voting Machine / Registration Systems*, Testimony for the Carter-Baker Commission on Federal Election Reform (Houston, Texas), June 2005.
70. Dan S. Wallach, *The Risks of Electronic Voting*, NSF Workshop on Cyberinfrastructure and the Social Sciences (Arlington, Virginia), March 2005.
71. Dan S. Wallach, *The Risks of Electronic Voting*, CASSIS: Construction and Analysis of Safe, Secure, and Interoperable Smart Devices (Nice, France), March 2005.
72. Dan S. Wallach, *The Risks of Electronic Voting*, University of Massachusetts, Amherst, Five Colleges Information Assurance Lecture Series (Amherst, Massachusetts), December 2004.
73. Dan S. Wallach, *The Risks of Electronic Voting*, University of Iowa, Department of Computer Science (Iowa City, Iowa), December 2004.
74. Dan S. Wallach, *The Risks of Electronic Voting*, CSI's 31st Annual Computer Security Conference (Washington, D.C.), November 2004.
75. Hans Klein, Eugene Spafford, Donald Moynihan, Dan S. Wallach, and Jim Reis, *Panel: E-Voting Policies and Perils*, Association for Public Policy Analysis and Management (APPAM) (Atlanta, Georgia), October 2004.
76. Dan S. Wallach, *The Risks of Electronic Voting*, Seventh Workshop on Languages, Compilers, and Run-time Support for Scalable Systems (Houston, Texas), October 2004.
77. Dan S. Wallach, *The Risks of Electronic Voting*, Symposium on the 2004 Presidential Election, John J. Marshall Law School (Chicago, Illinois), October 2004.
78. Chris Bell, Dan S. Wallach, and Tony J. Servello III, *Panel: Electronic Voting*, Science Café (Houston, Texas), October 2004.
79. Dan S. Wallach, *The Risks of Electronic Voting*, The Integrity of the Election Process, U. of Toledo Law School (Toledo, Ohio), October 2004.
80. Dan S. Wallach, *The Risks of Electronic Voting*, Princeton University, Department of Computer Science (Princeton, New Jersey), October 2004.
81. Dan S. Wallach, *The Risks of Electronic Voting*, DIMACS Workshop on Cryptography: Theory Meets Practice (Piscataway, New Jersey), October 2004.

82. Dan S. Wallach, Michael I. Shamos, Eugene Spafford, and Michael E. Lavelle, *Panel: Who Can Plug Into E-Voting Machines?*, E-lection 2004: Is E-Voting Ready for Prime Time?, John Marshall Law School (Chicago, Illinois), October 2004.
83. Dan S. Wallach, [Testimony for the NIST/EAC Technical Guidelines Development Committee](#) (Gaithersburg, Maryland), September 2004.
84. Dan S. Wallach, *The Risks of Electronic Voting*, DiverseWorks: The Voting Machine (Houston, Texas), September 2004.
85. Dan S. Wallach, *The Risks of Electronic Voting*, Baker Institute Forum on Electronic Voting (Houston, Texas), September 2004.
86. Dan S. Wallach, *The Risks of Electronic Voting*, League of Women Voters General Meeting (Houston, Texas), September 2004.
87. Dan S. Wallach, *The Risks of Electronic Voting*, Simposio acerca de Urnas Electrónicas para la Emisión del Voto Ciudadano (Mexico City, Mexico), September 2004.
88. Dan S. Wallach, *The Risks of Electronic Voting*, Fermi National Accelerator Lab (Batavia, Illinois), August 2004.
89. Dan S. Wallach, *The Risks of Electronic Voting*, TrueMajority "National Day of Action" (Austin, Texas), July 2004.
90. Dan S. Wallach, *The Risks of Electronic Voting*, 10th Annual County and District Clerks' Association of Texas Conference (Lake Conroe, Texas), June 2004.
91. Dan S. Wallach, *The Risks of Electronic Voting*, Texas State Democratic Party Convention, Progressive Populist Caucus (Houston, Texas), June 2004.
92. Dan S. Wallach, *Hack-a-Vote: Demonstrating Security Issues with Electronic Voting Machines*, DIMACS Workshop on Electronic Voting - Theory and Practice (Piscataway, New Jersey), May 2004.
93. Dan S. Wallach, [Testimony for the Texas Senate Committee on State Affairs](#) (Austin, Texas), May 2004.
94. Josh Benaloh, Dana DeBeauvoir, and Dan S. Wallach. *Panel: Electronic Voting Security*, IEEE Symposium on Security and Privacy (Oakland, California), May 2004.
95. Dan S. Wallach, *The Risks of Electronic Voting*, Harris County Democrats (Houston, Texas), April 2004.
96. Dan S. Wallach, *The Risks of Electronic Voting*, North Brazoria County Democrats (Pearland, Texas), April 2004.
97. Dana DeBeauvoir, Ann McGeehan, Dan S. Wallach, *Panel on the Security of Electronic Voting*, League of Women Voters (Austin, Texas), April 2004.
98. Dan S. Wallach, *The Risks of Electronic Voting*, Guest lecture in "Texas Political Parties and Elections" (Government 335N, University of Texas, Austin), March 2004.
99. Dan S. Wallach, [Testimony for the Texas House Elections Committee](#) (Austin, Texas), March 2004.
100. Dan S. Wallach, *The Risks of Electronic Voting*, Bell County Republican Convention (Belton, Texas), March 2004.
101. Dan S. Wallach, [Testimony for the Ohio Joint Committee on Ballot Security](#) (Columbus, Ohio), March 2004.
102. Dan S. Wallach, *The Risks of Electronic Voting*, Houston Peace Forum (First Unitarian Universalist Church, Houston, Texas), March 2004.
103. Ben Cohen and Dan S. Wallach, *TrueMajority Press Event* (Washington, D.C.) February, 2004.
104. Dan S. Wallach, *The Risks of Electronic Voting*, European Commission eDemocracy Seminar (Brussels, Belgium), February, 2004.

105. Dana DeBeauvoir, Dan S. Wallach, Ann McGeehan, Bill Stotesbery, Adina Levin, *Electronic Voting: Benefits & Risks*, First Unitarian Universalist Church of Austin (panel co-sponsored by Travis County Green Party and Austin Democracy Coalition) (Austin, Texas), January 2004.
106. Dan S. Wallach, *The Risks of Electronic Voting*, Texas IMPACT / United Methodist Women (Austin, Texas), January 2004.
107. Dan S. Wallach, *The Risks of Electronic Voting*, River Oaks Democratic Women (Houston, Texas), January 2004.
108. Dan S. Wallach, *The Risks of Electronic Voting*, University of Michigan, Department of Computer Science (Ann Arbor, Michigan), January 2004.
109. Dan S. Wallach, *The Risks of Electronic Voting*, EFF-Austin Policy Roundtable (Austin, Texas), December 2003.
110. Dan S. Wallach, *O.S. Security Semantics for Language-based Systems*, Katholieke Universiteit Leuven (Leuven, Belgium), December 2003.
111. Dan S. Wallach, *O.S. Security Semantics for Language-based Systems*, Belgium Java User's Group: JavaPolis (Antwerp, Belgium), December 2003.
112. Dan S. Wallach, *The Risks of Electronic Voting*, Austin Pastoral Center (Austin, Texas), November 2003.
113. Dan S. Wallach, *Peer-to-Peer Security*, Cornell University, Department of Computer Science (Ithaca, New York), November 2003.
114. Dan S. Wallach, *The Risks of Electronic Voting*, Duke University, Department of Computer Science (Durham, North Carolina), October 2003.
115. Dan S. Wallach, *The Risks of Electronic Voting*, University of Arizona, Department of Computer Science (Tucson, Arizona), September 2003.
116. Dan S. Wallach, *Peer-to-Peer Security*, [UW/MSR/CMU Software Security Summer Institute](#) (Stevenson, Washington), June 2003.
117. Dan S. Wallach, *Peer-to-Peer Security*, Stanford University, Department of Computer Science (Stanford, California), May 2003.
118. Dan S. Wallach, *Adventures in Copy Protection Research*, The Hockaday School (Dallas, Texas), April 2003.
119. Dan S. Wallach, *Adventures in Copy Protection Research*, Formal Techniques for Networked and Distributed Systems (Houston, Texas), November 2002.
120. Dan S. Wallach, *Peer-to-Peer Security*, Oregon Graduate Institute (Portland, Oregon), March 2002.
121. Dan S. Wallach, *Mobile Code Security Through Program Transformations*, Mathematical Foundations of Programming Semantics (New Orleans, Louisiana), March 2002.
122. Dan S. Wallach, *The Risks of E-Voting Machines*, Bay Area New Democrats (Houston, Texas), November 2001.
123. Dan S. Wallach, Testimony before the Houston City Council on the risks of electronic voting systems, July 2001.
124. Dan S. Wallach, *Adventures in Copy Protection Research*, Open Group Meeting (Austin, Texas), July 2001.
125. Dan S. Wallach, *Adventures in Copy Protection Research*, Houston Copyright Town Hall Meeting (Houston, Texas), April, 2001.
126. Dan S. Wallach, *Mobile Code Security Through Program Transformations*, U.C. Berkeley (Berkeley, California), March 2001.

127. Dan S. Wallach, *Mobile Code Security Through Program Transformations*, University of Texas (Austin, Texas), November 2000.
128. Dan S. Wallach, *Mobile Code Security Through Program Transformations*, International Workshop on Mobile Objects/Code and Security (Tokyo, Japan), October 2000.
129. Dan S. Wallach and John DeRose, *The Security of My.MP3.com and Other ``Beaming'' Technologies*, [MP3 Summit](#) (San Diego, California), June 2000.
130. Dan S. Wallach, *An Overview of Computer Security*, Law Practice Management Section of the Houston Bar Association (Houston, Texas), May 2000.
131. - Wallach has also spoken to visiting groups of high school students via a Rice outreach program organized by Jen Overton.

Advisees *Completed PhDs:*

Theodore Book (Square)
Scott Crosby (Two Sigma)
Mike Dietz (Google)
Judson Dressler (USAF)
Eyal de Lara (University of Toronto) (Prof. Willy Zwaenepoel was de Lara's advisor of record)
Tsuen Wan "Johnny" Ngan (Google)
Seth Nielson (Independent Security Evaluators)
Algis Rudys (Google)
Daniel Sandler (Google)
Anhei Shu (Google)

Completed Postdocs:

Peiyong Song (Google)

Completed Masters:

Anwis Das (Google)
Ersin Öksüzoglu (Intel)
Shashi Shekhar (Google)
Ping Tao (TI)

Current graduate & post-doctoral researcher collaborators:

Bumjin Im
Rabimba Karanjai
Jaeho Lee
Adam Pridgen
Daniel Song
Rima Tanash

Consulting *Private Consulting:*

[SRI International](#) (June 2016, computer security research)
[Solve Media](#) (March 2012, security architecture review)
[Authus](#) (May 2009, security architecture review)
State of California (Summer 2007, ["Top to Bottom" Voting System Review](#))
[AT&T Research](#) (Fall 2001, collaborating with Avi Rubin on security research)
[GalleryFurniture](#) (August 2001, post-attack web site audit and reinstall)
[Curl](#) (December 2000, security architecture review)
[Quaadros Technologies](#) (October 2000, design review)

[Cloakware](#) (September 2000 and August 2001, design review)

[Coral Technologies](#) (December 1999, security audit)

[MetaCreations](#) (March 2000, security audit)

[CenterPoint Ventures](#) (ongoing, technical evaluations of startups)

[Rho Ventures](#) (ongoing, technical evaluations of startups)

Legal Consulting (Election-related):

Jennings v. Buchanan (November 2006, expert for plaintiffs)

Conroy et al. v. Dennis (Colorado Sec. of State) (September 2006, expert for plaintiffs)

Santana et al. v. Williams (Texas Sec. of State) and DeBeauvoir (Travis County Clerk) (July 2006, expert for plaintiffs)

Taylor et al. v. Cortés (Pennsylvania Sec. of Commonwealth) (April 2006, expert for plaintiffs)

Bruni v. Valdes and Benavides (April 2006, expert for Bruni)

Flores v. Lopez (April 2006, expert for Flores)

ACLU v. Connor (Texas Sec. of State) (February 2005, expert for the ACLU)

Legal Consulting (Other):

Federal Trade Commission (July 2013)

Eolas v. Perot Systems (March 2011, expert for Perot Systems)

Bedrock v. Google (November 2010, consultant for Google)

TiVo v. AT&T (June 2010, expert for AT&T)

Finjan v. Secure Computing (August 2007, expert for Secure Computing)

Autobytel v. Dealix (May 2005, expert for Dealix)

Soverain v. Amazon.com (April 2005, expert for Amazon.com)

Uniloc v. Microsoft (November 2004, expert witness for Microsoft)

Nash v. Microsoft (May 2004, expert witness for Microsoft)

Recruitsoft v. Hire.com (August 2003, expert witness for Hire.com)

DirecTV v. NDS (April 2003, expert witness for DirecTV)

RIAA v. MP3.com (February 2000, wrote declaration for MP3.com)

Employment [Rice University](#), Professor, [Department of Computer Science](#), beginning October 1998.

History (Promoted from assistant professor in May 2005; promoted from associate professor in 2012.)

1/07 - 12/07 [Stanford University](#), [Department of Computer Science](#), visiting professor / [SRI Computer Science Laboratory](#), visiting researcher

9/93 - 10/98 [Princeton University](#), Graduate student, [Department of Computer Science](#). Supported by grants from NSF, Sun Microsystems, Intel, Microsoft, and others.

6/97 - 8/97 [Netscape Communications Corporation](#), Mountain View, California.

Integrated Java with SSL. Audited the CORBA and RMI implementations for security bugs. Wrote a CORBA demonstration (a chat server).

6/96 - 8/96 [Netscape Communications Corporation](#), Mountain View, California.

Designed and implemented a privilege-based security mechanism and user interface to enable digitally-signed Java applets. Participated in design reviews of several Netscape and JavaSoft technologies.

6/95 - 8/95 [Microsoft Corporation](#), Redmond, Washington.

Wrote a converter from Softimage to a RenderMorphics-based system ([V-Chat](#)). Designed and implemented a polygonal model compression system for virtual reality applications.

6/94 - 8/94 [David Sarnoff Research Center](#), Princeton, New Jersey.

Wrote a microcode-level simulator for parallel video processing engine. Wrote design documents for the client side of a future video-on-demand system.

6/93 - 8/93 [Berkeley Systems](#), Berkeley, California.

Ported a screen-reading system (allowing blind people to use graphical user interfaces) from Microsoft Windows to X.

9/92 - 6/93 [U.C. Berkeley](#), Research Assistant for Dr. Larry Rowe.

Implemented parts of a MPEG-1 video encoder. Wrote the audio support for a real-time distributed media-on-demand system.

EXHIBIT B: Testimony before the U.S. House's Space, Science, & Technology Committee

Testimony of Dr. Dan S. Wallach
Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy
Rice University, Houston, Texas

Before the House Committee on Space, Science & Technology Hearing,
“Protecting the 2016 Elections from Cyber and Voting Machine Attacks”

September 13, 2016
Rayburn House Office Building, Room 2318

Chairman Smith, Ranking Member Johnson, members of the committee, it's an honor to speak to you today about our nation's voting systems, the potential threats they face this November, and the steps we might take to mitigate these threats.

My name is Dan Wallach. I've been a professor of computer science at Rice University, in Houston, Texas, for 18 years. My research considers a variety of computer security topics and I've published over 100 papers in the field. Among other honors, I recently served from 2011-2015 on the Air Force Science Advisory Board. I've included a more detailed biography in my written materials. My main message for you here, today, is that our election systems face credible cyber-threats; it's prudent to adopt contingency plans before November to mitigate these threats.

I've maintained a research interest in electronic voting systems starting with their widespread adoption in the early 2000s. In particular, I led an NSF-funded research center, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections)¹ from 2005-2011. I also participated in the 2007 California "Top to Bottom Review" of its electronic voting systems, where we found unacceptable security vulnerabilities in every system we studied²; those systems were replaced in California with more secure, paper-based systems but are still being used elsewhere and are likely still quite vulnerable. One of my ongoing projects is helping the Travis County (Austin, Texas) Clerk's office design a new electronic voting system to replace their current, aging system³. In short, my experience makes me very familiar with how our election systems are vulnerable and how our adversaries might seek to exploit them.

First, I'd like to address the threat. We've learned that foreign nation-state actors, likely Russian, broke into DNC computers and released documents for expressly partisan purposes⁴. So far as we know, they're doing this to manipulate the outcome of November's election. We must ask ourselves the same sorts of questions that arise in any security analysis. Does the adversary have the *means*, *motive*, and *opportunity* to have their desired effect, and do we have the necessary *defenses* and/or *contingency plans* to mitigate these threats?

¹ <http://accurate-voting.org/>

² <http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/>

³ <https://www.usenix.org/conference/evt2013/workshop-program/presentation/bell>

⁴ See, e.g., Lichtblau's article in the *New York Times* (July 29, 2016).
<http://www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html>

It's important to note that this has happened in elections before. Russian hackers, who may or may not have been government-affiliated, committed "wanton destruction" upon Ukrainian election systems in 2014, arranging for the vote tallying system to report incorrect results⁵. The Ukrainians were lucky to catch this; it's not uncommon for nation-state computer attacks to go unnoticed for months or years. Like the Ukrainians in 2014, we face similar vulnerabilities today.

I've written about these issues in a detailed series of blog posts⁶ which I'll summarize for you here. **Our biggest vulnerabilities are our voter registration databases**, typically maintained online, so therefore reachable by our adversaries. Web sites with databases are ubiquitous and their vulnerabilities are well-understood to cyber threat actors. Every university computer security class has its students learn to attack and defend these sorts of things. While a defender must eliminate all possible attacks, an attacker needs only find a single weakness, so it's reasonable to expect these weaknesses exist in our voter registration systems. **We can and should expect our adversaries to go after voter registration systems**, and there's evidence of this already having happened in Arizona and Illinois^{7 8}. The partisan impacts are easy to envision. You can selectively disenfranchise voters by deleting them from the database or otherwise introducing errors. How can you infer voter partisanship? Political campaign managers use a variety of predictive models for targeted mailings, get-out-the-vote campaigns, and so forth; we can expect adversaries to do the same. **Can we mitigate against these threats?** First and foremost, we can require computer backups and run drills to make sure we can rapidly recover from corruption. To detect and deter more sophisticated adversaries, we should deploy state-of-the-art intrusion detection and prevention systems in "battleground" counties and states. Furthermore, we already have "provisional voting," allowing voters to cast a ballot, despite their absence from the database, but provisional voting procedures are meant to handle a fairly small number of voters. If a substantial fraction of voters had to vote provisionally, doing the necessary paperwork, the process would grind to a halt. Long lines disenfranchise voters. Provisional balloting also doesn't work very well in states heavily

⁵ Clayton, "Ukraine election narrowly avoided wanton destruction from hackers", *Christian Science Monitor* (June 2014), <http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video>

⁶ <https://freedom-to-tinker.com/blog/dwallach/election-security-as-a-national-security-issue/> and <https://freedom-to-tinker.com/blog/dwallach/a-response-to-the-national-association-of-secretaries-of-state/>

⁷ Isikoff, "FBI says foreign hackers penetrated state election systems", *Yahoo! News* (August 29, 2016), <https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html>

⁸ Nakashima, "Russian hackers targeted Arizona election system", *Washington Post* (August 29, 2016), https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html

utilizing vote-by-mail ballots (e.g., California, Colorado, Nevada, Oregon and Washington State), where voters might not even realize their ballots are missing. We might be able to use traditional printed paper pollbooks, rather than electronic pollbooks, but these don't work easily with either early voting or election day vote centers, where many thousands of different ballot styles must be available to thousands of voters.

Can our adversaries get malware into our voting machines, themselves? The U.S. military protects its important secrets by keeping them on distinct networks and servers, physically separated from the Internet. This "air gap" defense is also used to protect voting machines. Despite this, voting machines still interact with normal computers as part of their initialization phase (loading software and ballot definitions) and the tabulation phase (extracting cast-vote records and computing the totals). Even if the whole process is designed to be "air gapped" from the Internet (and it absolutely must be air-gapped), nation-state adversaries have devised a variety of workarounds. The Stuxnet malware, for example, was engineered specifically to damage nuclear centrifuges in Iran, even though those centrifuges were never connected to the Internet. We don't know exactly how the Stuxnet malware got in, but it did nonetheless⁹. Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems, and especially if we consider the possibility of insider threats, then yes, it's entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries' capabilities. The best mitigations we have for systems that we use today are only feasible where we have paper ballots. The mere *possibility* of a recount or audit of the paper ballots acts as a deterrent to an electronic attack; it's much more difficult to tamper with paper, in bulk, relative to the effort to tamper with purely electronic records, as used in a number of states including the battleground states of Pennsylvania and Georgia. Conversely, if our paperless electronic voting systems were attacked, we'd be unlikely to see evidence of it in the voting machines or tally systems.

Does an adversary need to attack everywhere? Our adversaries understand how the American political system works. They know about "battleground states". They can focus their efforts on states where a small nudge might have a large impact. Also, consider that our adversaries might have a variety of goals. If they simply want to disrupt our elections, and if they're unconcerned with attribution, then even very modest or crude attacks will raise doubts and damage voter confidence in the election outcome. Trust in our election systems is fragile and is potentially easily shaken by our adversaries.

⁹ For more details, see, e.g., Langner et al. (2013).
<http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>

What can we do between now and November? It's far too late to change the technologies upon which we will cast our votes. My best advice is that we need *contingency planning*. Four years ago, when Hurricane Sandy disrupted elections in several northeastern states, this was a big topic of discussion¹⁰. The National Association of Secretaries of State prepared a summary of relevant statutes in every state¹¹. In many respects, cyber activities from a nation-state adversary are similar to natural disasters in the impact they can have on our elections. What can you do if your voter registration database has been destroyed? Perhaps try to restart things from a backup. What can you do if your electronic voting systems refuse to turn on? Perhaps make an advance arrangement with a print-shop to rush a large order of paper ballots if need be. What if we have no direct evidence of tampering but we have credible intelligence reports that suggest otherwise? Many state statutes already allow governors to declare states of emergency and take appropriate actions up to and including re-running the election on a different day. In short, we must prepare for a disaster, while hoping it may never occur.

When we talk about nation-state adversarial attacks on computer networks, we often use the term "advanced persistent threat" (APT), indicating that these adversaries are good at hiding and at sticking around despite efforts to remove them. While it's helpful and important to apply software updates, use good passwords, properly configure firewalls and intrusion detection systems, and otherwise practice "good hygiene", the process of detecting and removing an APT adversary is complicated. A number of companies and consultancies have begun offering products and services that help in this area, and state and county office should hire such companies to audit and remediate their systems, particularly in "battleground" states, although this may require financial assistance from the Federal government.

How do we make sure we won't face these risks in subsequent elections? The 2002 Help America Vote Act had two parts. It allocated money to replace obsolete voting equipment and it created the Election Assistance Commission (EAC) which, among other things, absorbed the voting systems standards-making process which was previously managed by the National Association of State Election Directors (NASD). The problem was that the money was allocated to the States before the EAC was up

¹⁰ See, e.g., Kaplan in the *New York Times* (November 12, 2013) <http://www.nytimes.com/2013/11/13/nyregion/lessons-from-hurricane-sandy-being-applied-to-election-planning.html>

¹¹ <http://www.nass.org/elections-voting/nass-task-force-on-emergency-preparedness-for-elections/>. See also, Wall, *Preventing Disasters from Disrupting Voting: National Task Force Urges States To Plan for Election Emergencies* (October 15, 2014) <http://knowledgecenter.csg.org/kc/content/preventing-disasters-disrupting-voting-national-task-force-urges-states-plan-election>

and running; the vendors who had products for sale at the time were able to sell these inadequate products as-is and had neither the incentives nor ability to improve them. Now, a over decade later, many of these systems are nearing the end of their usable service life. Their aging hardware is starting to break down. What should we buy next time to make sure we don't have these problems again? I see two options:

Next-generation optical scan systems: The big elections equipment vendors are all now selling “precinct-based optical scan systems” (PCOS), as shown in Fig. 1, where paper ballots are marked by hand and scanned at the ballot box. These systems offer features to catch some kinds of voter errors¹², allowing voters a chance to remake their ballot. Optical scan systems face all the same electronic tampering threats from adversaries, but these threats can be mitigated by robust paper auditing procedures. California piloted such audits in 2011-2013 and submitted a variety of recommendations to the EAC¹³, presently also part of California and Colorado state laws. In short, by randomly selecting a small number of paper ballots and comparing those to their corresponding digital records, you can mathematically determine that if you were to actually do a full recount -- that is, count all the paper ballots -- the results would not differ between a hand count and the electronic count. Not only does this help with accuracy, it also mitigates against malicious software tampering, because such tampering would introduce discrepancies that the audit would detect.



Fig. 1: ES&S DS200, precinct-based optical scanner with on-screen assistance features.

¹² The two primary forms of “voter error” that we can detect in a scanner are “overvotes”, wherein a voter selects more than one candidate for a given election contest, and “undervotes”, wherein a voter selects no candidates for a given contest.

¹³

<http://www.sos.ca.gov/elections/voting-systems/oversight/post-election-auditing-regulations-and-reports/post-election-risk-limiting-audit-pilot-program/>

Next-generation hybrid voting systems: The two most exciting developments aren't coming from the commercial voting system vendors but instead from election officials in Los Angeles County, California and Travis County (Austin), Texas. The LA Voting Systems Assessment Project (VSAP)¹⁴, as seen in Fig. 2, and the Travis County STAR-Vote (Secure, Transparent, Auditable, Reliable) system¹⁵ both use large touch-screen computers which can accommodate complex ballot designs with multiple languages and both offer sophisticated accessibility features. Both generate printed paper ballots which can be tallied electronically and audited manually. Both use sophisticated cryptographic techniques to protect the system.



Fig. 2: Los Angeles VSAP prototype, with button-box, touch-screen, and printer.

I've been working more closely with Travis County than Los Angeles, so I can tell you that Travis County has allocated \$4 million to start their procurement process shortly; they expect they will ultimately spend around \$12 million before they can begin testing in real elections in 2019. If they had additional funds now, they could advance their timeline and have a more full-featured system.

Both Travis and Los Angeles Counties envision their systems will use open source software, reducing ongoing support and maintenance costs. These projects have the potential to see widespread nationwide

¹⁴ <http://vsap.lavote.net/>

¹⁵ <http://traviscountyclerk.org/eclerk/Content.do?code=E.34>

adoption, which would make elections far more resilient to cyber attacks than with the voting systems currently on the market.

Internet voting: While it's not directly relevant to today's hearing, somebody will inevitably propose Internet voting as a solution to every problem in voting.

Why can't we just vote on the Internet? While it's attractive to imagine the convenience of online voting, the Internet also makes it much easier for nation-state adversaries to attack our elections. In one prominent example, Washington DC conducted a pilot election using an Internet voting system, inviting external researchers to have a go at attacking them. The University of Michigan's Prof. Alex Halderman and his students managed to completely compromise this system in a few hours¹⁶. They were able to watch election workers from the internal video cameras. They arranged for fictional characters to win all the elections. They even modified the web site to play the Michigan fight song after each vote was cast. If Prof. Halderman and his students can do this, so can our adversaries. Halderman and others have studied Internet-based voting systems in New South Wales, Australia¹⁷, and in Estonia¹⁸, finding similar problems. Safe internet voting is simply not feasible today. Instead, we need paper ballots or hybrid systems.

But we can do banking on the Internet! Companies that engage in electronic commerce make significant, ongoing investments in the security of their operations. Despite those investments, their losses are significant:

In 2015, the British insurance company Lloyd's estimated that cyber attacks cost businesses as much as \$400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts over the past year put the cybercrime figure as high as \$500 billion and more.¹⁹

¹⁶ Wolchok et al., "Attacking the Washington D.C. Internet Voting System", Proc. 16th Conf. on Financial Cryptography & Data Security (February 2012), <https://jhalderm.com/pub/papers/dcvoting-fc12.pdf>

¹⁷ Halderman and Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election" (June 2015), <http://arxiv.org/abs/1504.05646>

¹⁸ Springall et al, "Security Analysis of the Estonian Internet Voting System", ACM CCS (Nov. 2014), <https://jhalderm.com/pub/papers/ivoting-ccs14.pdf>

¹⁹ Morgan, "Cyber Crime Costs Projected To Reach \$2 Trillion by 2019", *Forbes* (Jan. 2016), <http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/>

We can't afford fraud in elections. We can't simply write it off as a cost of doing business. Furthermore, in banking, if a fraudulent transaction occurs, perhaps because a credit card number was stolen, the victim will see it on their statement and can dispute it. In sharp contrast, if an Internet vote was flipped, current systems give the voter no evidence with which discover this. (We don't want voters to have "receipts" indicating how they voted, because that would enable bribery and coercion. Voter privacy is necessary for a secret-ballot election.)

*Will we **ever** be able to vote on the Internet?* Eventually, yes, but definitely not with today's computers, and not on today's internet. This is an open research challenge which requires better security across the board, from consumer operating systems and web browsers through our networks and cloud infrastructure. Internet voting is a great aspirational goal, but it's not feasible yet to do this, particularly in light of the threats these systems will face.

Can't we use sophisticated cryptography, as in the Bitcoin blockchain? Bitcoin is an electronic currency with a global "shared ledger" that has some interesting security properties. Some people have even proposed that we can use it to cast ballots, since casting a ballot for a candidate is superficially similar to sending a "coin" to that candidate. This isn't the venue for a detailed technical critique, but suffice to say that we've included blockchain-like techniques in Travis County's STAR-Vote, and that cryptographic techniques don't magically eliminate the dangers of having a voting system online and accessible to our nation-state adversaries. Furthermore, it's important that our election integrity not rely solely on intangible mathematics. There must also be tangible evidence that can be understood without an advanced degree. That tangible evidence must be paper ballots.

How can we better enable our overseas and military voters to cast their ballots? Many overseas voters complain that postal ballot delivery and return is slow and unreliable. The current state of the art process is delivering ballots digitally where the voter prints them, marks them by hand, and returns them in the postal mail. In some cases, military ballots are returned by fax, printed, and then mailed domestically. This process is a mess and we owe a better solution to our overseas and military voters. Rather than Internet voting, what we really need is some form of *remote kiosk voting*, where overseas voters can go to a nearby embassy, consulate, or military base. There's a clear role here for NIST and the EAC to standardize these things, making it easier for a remote voter to cast a private vote in a controlled polling location.

Conclusions

As Don Rumsfeld once said, “you go to war with the army you have, not the army you might want or wish to have at a later time.” We face a similar situation this November with our systems for voter registration, casting, and tabulation. None of them are ready to rebuff attacks from our nation-state adversaries, nor can we replace them in time to make a difference. Despite this, we can pursue a number of pragmatic steps, such as verifying the integrity of election database backups, and we can make contingency plans for how we may respond if and when we do detect attacks against our elections. If we can somehow determine that tampering with an electronic voting systems took place, we should have plans in place to rapidly print paper ballots and bring the voters back to the polls. The sooner we can create and agree on such plans, the more resilient our elections will be to foreign attacks. And even if nothing goes wrong and all this turned out to be nothing but hot air, we should treat these events as a warning. With modest investments, we can improve our practices and replace obsolete and insecure equipment, defeating future attacks like this before they ever get off the ground.

One Page Summary

Our elections face a credible threat. We've learned that Russia may have been behind leaked DNC emails, explicitly to manipulate our elections. We've also learned of attacks on voter registration databases in Arizona and Illinois. We must prepare for the possibility that sophisticated adversaries will use their "cyber" skills to attack our elections. And they need not attack every county in every state. It's sufficient for them to go after "battleground" states, where a small nudge can have a large impact.

Voter registration databases are particularly vulnerable because they're online. If an attacker can damage or destroy our voter registration databases, they could disenfranchise significant numbers of voters, leading to long lines and other difficulties.

Paperless electronic voting systems, and their tabulation systems, are also vulnerable. Despite not generally being connected to the Internet, these systems were never engineered with security in mind, and expert analyses have found unacceptable security issues. Our biggest nation-state adversaries have the capability to execute attacks against these systems.

Our options between now and November are largely limited to contingency planning. If we're lucky, we might detect attacks before Election Day, but it's important to make plans for recovering from unforeseen cyber disasters in the same way that we make plans for natural disasters, including running drills and exercises. If, for example, we were to conclude that our computer systems were unreliable, a contingency plan might be to rapidly print millions of paper ballots and rerun the election. Legislation passed in most states following 2012's Hurricane Sandy generally allows for such mitigations.

We must also plan for the next few years, after November's election is complete. Roughly one third of American voters this fall will use aging electronic voting systems with proven insecure designs. New hybrid voting systems, with electronic user interfaces and printed paper ballots, are being designed by Los Angeles County, California and Travis County (Austin), Texas. These have the potential to substantially reduce costs and improve the security of our elections. Federal support could advance their deployment nationwide. If we do nothing, keeping our aging systems in service holds our elections at risk.

Our immediate future should not include Internet voting. It's hard enough to protect the online systems that we already have. Moving additional voters online will only make things worse. Traditional, hand-marked paper ballots and the new hybrid electronic systems are our best paths forward.

Biography

Dan S. Wallach is a Professor in the Department of Computer Science and a Rice Scholar at the Baker Institute for Public Policy at Rice University, where he has been for 18 years. His research considers a variety of topics in computer security, including electronic voting systems security, where he served as the director of an NSF-funded multi-institution research center, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), from 2005-2011. He has also served as a member of the Air Force Science Advisory Board (2011-2015) and the USENIX Association Board of Directors (2011-2013).

Wallach earned his M.A. (1995) and PhD (1999) from Princeton University, advised by Profs. Edward Felten and Andrew Appel. He earned his B.S. EE/CS from the University of California, at Berkeley (1993).

EXHIBIT C: Answers to Post-Testimony Questions

Written Q&A for Dr. Dan S. Wallach
Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy
Rice University, Houston, Texas

Following the House Committee on Space, Science & Technology Hearing,
“Protecting the 2016 Elections from Cyber and Voting Machine Attacks”

Hearing date: September 13, 2016

Questions submitted by Rep. Lamar Smith

1. How would you rank the vulnerability of the following: paper ballots, electronic voting machines with a paper ballot trail, electronic voting machines without a paper ballot trail, optical scan systems, and Internet voting?

From worst to best: Internet voting, electronic voting without a paper trail, electronic voting with a paper trail, paper ballots (centrally tallied), paper ballots with a precinct-based optical scanner.

Internet voting, in all of its current commercial forms, is not suitable for use in Federal elections. Given our understanding of the capabilities of the nation-state adversaries that an Internet voting system might face, we cannot guarantee the integrity and privacy of the vote, nor can we ensure the availability of the infrastructure supporting an Internet election.

The rest of my ranking generally favors paper ballots, with an extra edge to paper ballots which are scanned and tabulated in the local precinct. This configuration creates electronic records, suitable for rapid election night results. Furthermore, by having redundant electronic and paper records, we can conduct post-election audits that can detect (and thus deter) ballot-box stuffing or electronic data tampering.

2. Is the diffusion of our voting infrastructure across 50 states and nearly 10,000 localities a substantial impediment to cyber-attacks and hacking?

While this is an important benefit to the security of our election systems, there are a small number of vendors whose voting systems and/or voter registration database systems are widely used. An attack that was engineered to compromise one such system would be likely to work against other copies of the same system. Furthermore, an adversary who wished to tamper with our nation's elections need not tamper with each and every locality in order to flip the outcome. We would expect such adversaries to focus their efforts on battleground states, particularly the largest counties in those states where more votes are cast.

3. It has been said that a graduate student in computer science could figure out how to hack into an electronic voting machine. Do you believe that this is something that could happen this upcoming election, with the student's actions leading to a change in an election result?

Prior studies of election security sponsored by the states of California, Ohio, and Florida were conducted by a mix of industrial professionals, professors, and graduate students. Based on the findings of these studies, and my participation in the California Top to Bottom Review, I

estimate that an engineering team of this sort with access to working voting machines, but not given access to the source code to those machines, would require roughly 6 man-months of effort to discover relevant vulnerabilities and craft suitable cyber-attack tools. Once such tools were crafted, the next challenge would be inserting them into a live election. The details for how to do this would obviously vary from one system to another, but would be greatly aided by the common practice of election officials staging their equipment in the field in advance. (This is colloquially referred to as the “sleepover problem”, and is a direct consequence of the logistical challenges of managing the distribution of election equipment.)

4. What do you suggest is the most important thing that the states can do between now and the November elections to ensure that voting runs as smoothly as possible?

I have two specific recommendations. First, states and counties should request the assistance of federal cyber-investigators from DHS, FBI, and other such agencies, or from private companies that similarly specialize in auditing computer networks for intrusions. If lucky, they may discover latent attacks prior to the election, allowing for the possibility of specific pre-election mitigations. But, in the event that nothing is found, my second recommendation is for states and counties to produce detailed contingency plans for how they may recover from a “cyber disaster”, should it occur. Having such plans, detailed in advance and agreed to by all parties, might dissuade attackers, knowing that the impact of their cyber attacks would be mitigated.

5. How can we better enable our overseas and military voters to securely cast their ballots?

My preference is that overseas and military voters be provided with “kiosk” polling places in embassies, consulates, and military bases. The design of a voting kiosk might be very similar to the design of a traditional polling-place voting system, except the return of voted ballots would be more complicated. Such a system might return ballots simultaneously through a combination of electronic means (using sophisticated cryptography) and traditional means (overnight couriers, etc.). Doing this properly requires having standards for how data is exchanged---a requirement where NIST has a natural role to play. We’re still many years away from this being a reality.

At present, it should be noted that with the passage of the Military and Overseas Voter Empowerment (MOVE) Act in 2009, the “time and distance” problem for military voters has been greatly mitigated without requiring that voters risk secrecy and security by sending voted ballots over the Internet. Local election officials send requested ballots 45 days in advance of Election Day, voters can receive blank ballots electronically that same day, and military voters can use a special return label for trackable express ballot return that typically gets voted ballots back to the county official in 5-6 days. Half the states allow late-arriving military ballots to be counted if sent in a timely fashion.

6. Is there a way that we can use sophisticated cryptography, such as blockchain, to submit secure votes?

Cryptographic block chain technologies are an important ingredient in the design of secure electronic voting technologies. However, they do not represent a “silver bullet” with respect to solving all of the problems that arise with Internet voting. We simply do not have all the necessary technologies to guarantee voter privacy, ballot integrity, and election availability in the face of a determined adversary. I estimate that we are at least ten years away from the possibility of such a system, with significant unsolved and open research challenges standing between us and any such system being suitable for real-world use.

7. Is there enough research and development being undertaken in the security of voting and election systems?
 - a. What technological areas should NIST prioritize in order to strengthen election cybersecurity?

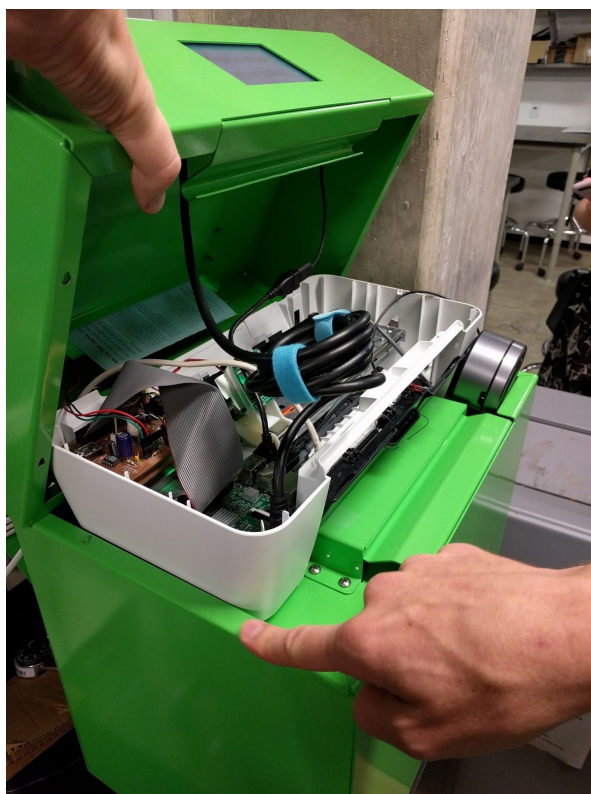
The National Science Foundation supports my own research in this area, as well as that of many of my colleagues, but there are no large efforts akin to DARPA’s “grand challenges” being pursued at this time by any Federal agencies. The two most promising efforts, at the present time, are being pursued by Los Angeles County, California and Travis County (Austin), Texas. I’m personally engaged with the Travis County effort, and my understanding is that Federal funding could significantly accelerate their development process, which would yield an “open source” implementation that could then be shared with other counties and states.

NIST and the EAC can play an important role in ensuring that the technologies developed in LA and Travis counties be suitable for other counties and states, both by directly funding these efforts (and, thus, accelerating their development) and by identifying other counties and states who might be amenable to adopting these new systems, collecting and organizing their requirements such that the development efforts will address them. Furthermore, they can ensure that the voting system standards, currently being updated, avoid presenting unnecessary barriers to these new machines, while raising the bar to rule out the older generation of insecure devices.

8. Given the criticisms you and others have made about the security of voting machines, going so far as to call the coding in one particular manufacturer’s machine “unacceptable”, should more stringent testing have been conducted of these machines by either NIST or the EAC prior to approval for use by states?

The current “voluntary voting system guidelines” have the conundrum of making very detailed requirements of vendors’ systems, while making negligible requirements of vendors’ engineering processes. Problems that are only discovered late in the engineering process are more expensive to fix, particularly if those problems are a result of poor engineering decisions made early in a system’s design process. This is a recognized issue when attempting to build secure systems *and* while trying to build usable systems. Waiting until the very end to evaluate the result is not the way to achieve security *or* usability.

In contrast, Travis County envisions that their procurement process will result in two performers under contract: a development organization and a “red team” organization. The “red team” will be responsible for attacking the system at every stage of its design and development, ensuring that major architectural problems are discovered and remedied early, when they’re cheaper to remedy. We’re already doing usability studies on mockups of the system at Rice University which will inform the ultimate designs. Below are two photos of our second-generation prototype ballot box, one showing the voter’s experience and another showing the internal paper-handling mechanisms (here, derived from an HP inkjet printer, with the printing parts removed; the whole thing is driven by a Raspberry Pi embedded computer and a variety of cheap accessories, including a laser barcode scanner).



9. The media has made much about the potential of a foreign-nation threat to the 2016 elections, but what about domestic threats: are home-grown hackers also a potential threat for the upcoming elections?

To date, there has been no public evidence of domestic threats of this magnitude. Regardless, foreign nation-state adversaries represent a “worst case” scenario. Any mitigations we might take against foreign adversaries will also protect us against hypothetical domestic threats.

10. Elections typically bring about stories and allegations about one political party trying to manipulate the system in their candidate’s favor. Is it conceivable that such action could extend to one part electronically attacking or attempting to hack into voting and election systems to benefit their candidate of choice?

The notable difference between threats abroad and threats domestic is that any analysis of domestic threats must necessarily consider *insider threats*, wherein a poll worker or election official might value their personal partisan preference over their professional non-partisan duty. Generally speaking, when we consider foreign adversaries and their capabilities, we already must consider insider threats, wherein a poll worker or election official might be bribed or otherwise recruited by the foreign adversary.

The main practical impact of insider threats is that we cannot assume that an “airgap” defense is sufficient. A robust voting system must remain robust even in the face of threats from within.

11. In retrospect, has HAVA been a net plus or net minus?

HAVA was a huge benefit to our nation’s elections, retiring old and obsolete lever and punchcard systems, and creating the EAC to manage standards and processes. HAVA’s greatest failing was disbursing money to purchase new equipment before the EAC and its processes had a chance to even get started. This led us to the present-day situation where expensive equipment, purchased with HAVA, is now aging and obsolete, and was never engineered against an appropriate security model. Sadly, when the EAC tried to add even modest security and other updates to the VVSG requirements, the vendors found the process cumbersome and largely abandoned their products rather than updating them.

As described above (answer to question 8), it’s expensive and difficult to add requirements to a complete product, especially when those requirements are best met by changing the entire development process. Conversely, if we had good standards and processes in place *before* the vendors began their work, we’d have equipment that was more usable, more secure, and we

could have made it easier to mix-and-match equipment. Good standards help prevent vendor lock-in, and that in turn, can improve pricing and features in the market.

12. Some experts have stated that the paper ballot is in and of itself secure. Do you agree with that statement?

The best security comes from having *copies* that have different failure modes. A precinct-based optical scanner creates electronic copies of ballots as they are deposited in the ballot box, meaning that post-election stuffing of paper won't be reflected in the electronic records, nor will post-election electronic tampering be reflected in the physical box of paper ballots. An attacker would need to consistently tamper with both paper and electronic records--a significantly harder job than tampering with either one alone. It's worth noting that the security in a scheme like this comes from a *mandatory auditing process*, as part of the post-election "canvass" period prior to the election results being certified. Evidence that's not considered provides no security benefit.

When we envision a sophisticated nation-state adversary engineering custom-built exploits for purposes of attacking an election, we have to consider the very real possibility that all of the electronic records resulting from an election might be tampered. This is where printed paper ballots, *in addition to those electronic records*, provide the strongest possible security model. Once printed, they cannot be "un-printed", particularly if their chain of custody is protected through simple, traditional means (e.g., video cameras, security guards, locked vaults).

The Travis County design, in particular, creates cryptographic "receipts", printed on paper, that voters can take home which allow them to cryptographically *prove* that their ballots were not tampered as part of the tally, while not being able to prove to anybody else how they avoided¹. There are even mechanisms to detect if a machine tried to cheat a voter and record a vote differently from the voter's intent. These sophisticated cryptographic mechanisms work hand-in-hand with printed paper ballots, producing election results that are stronger than cryptography or paper, alone, might accomplish.

¹ We cannot allow voters to take home any sort of receipt that indicates their vote selections, because that would enable bribery and coercion. "Vote for my candidate and I'll pay you \$20". When we speak of a "cryptographic receipt", we mean that it prevents this sort of bribery and coercion while still allowing other useful properties to be proven by the voter or by any organization acting on the voter's behalf.

Question submitted by Rep. Eddie Bernice Johnson

1. In response to a recommendation by the Presidential Commission on Election Administration, the CalTech/MIT Voting Technology Project developed a web site that election officials can use to determine if they can deploy a more efficient line management configuration to help shorten lines. The project highlighted the science of line management and queuing theory. What other areas of election and voting science and technology should Congress, particularly this Committee, look to support?

The broad challenge of improving our nation's elections requires not only *secure* voting systems, but also *usable* voting systems. My research involves extensive collaboration with human factors experts to ensure that our security mechanisms don't have a negative impact on voter speed, accuracy, and satisfaction. NIST has a lot of usability expertise, and they've supported some of my colleagues' usability studies on voting. Additional NIST engagement on this issue would be beneficial for studies of all the nuts-and-bolts issues in elections (e.g., poll worker training effectiveness).