Testimony of Dr. Dan S. Wallach

Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy
Rice University, Houston, Texas

Before the Texas Senate Select Committee on Election Security

February 21, 2018
Texas Capitol Extension, Hearing Room E1.012

Chairman Hughes, members of the committee, it's an honor to speak to you today about our nation's voting systems, the potential threats they face in modern elections, 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 20 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 and we need to take steps to mitigate those 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) 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 studied[1]; those systems were replaced in California with more secure, paper-based systems but are still being used elsewhere, including here in Texas, and appear to be still unacceptably vulnerable. One of my recent projects was helping the Travis County Clerk's office design its STAR-Vote system, a new electronic voting system with strong security designed in from the beginning[2], which I'll talk about more later in my testimony. In short, my experience makes me very familiar with how our election systems are vulnerable and how our adversaries might seek to exploit them.

In September 2016, I was asked to testify in front of U.S. Congress's Committee on Space, Science, and Technology on this same topic. My testimony today includes many of the same things I said then, with some updates on what we've learned since then.

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 purposes[3]. This was clearly part of

[1] http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/
[2] https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell
[3] 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

their larger effort, including the social media manipulation that we're reading about in recent news[4]. In a Senate Intelligence Committee hearing just last week, Dan Coats, the director of national security, stated "We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople and other means of influence to try to exacerbate social and political fissures in the United States."[5] With respect to our election systems themselves, Jeanette Manfra, an official at DHS stated, "While scanning and probing of networks happens across the internet every day, we have not seen specific or credible evidence of Russian attempts to infiltrate state election infrastructure like we saw in 2016."[6] Ms. Manfra also stated that "21 officials in 20 states" now have secret-level clearances for receiving DHS threat briefings.[7]

Given the interest of a hostile nation-state in our own elections, 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?

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 results[8]. 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 Ukranians in 2014, we face similar vulnerabilities today.

I've written about these issues in a detailed series of blog posts[9] 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

---

[4] See, e.g., Shane, "How Unwitting Americans Encountered Russian Operatives Online", *New York Times* (February 2018), https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html

[5] See, e.g., Rosenberg, Savage and Wines, "Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn", *New York Times* (February 2018). https://www.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html

[6] *Ibid*.

[7] *Ibid*.

[8] 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

[9] 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/

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 and Illinois[10] [11]. 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. We must certainly establish baseline computer security standards for network firewalls, intrusion detection systems, and other "good hygiene" practices, along with state resources to help our counties adopt such practices.

Worst case, we 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 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" style of 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

[10] 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
[11] 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

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 nonetheless[12] . 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.

Most Texas counties are using equipment that's over a decade old[13], which means that we must assume that our adversaries have had the time to devise attacks. We currently rely on physical protections to defend our systems, and that is no longer enough. On top of all that, just by virtue of its age, this equipment will need to be replaced. It's time to plan for the necessary expenses, and to ensure that the next round of equipment satisfies better security standards.

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, and that applies at the local level as well. We have several interesting Congressional races coming up this November in Texas, any one of which could be subject to overseas attention. 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.

---

[12] For more details, see, e.g., Langner et al., "To Kill A Centrifuge" (2013). http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[13] Rabinowitz, "Election Security a High Priority - Until It Comes to Paying for New Voting Machines", *ProPublica* (February 2018) https://www.propublica.org/article/election-security-a-high-priority-until-it-comes-to-paying-for-new-voting-machines

What can we do between now and November? I first wrote this paragraph in September 2016, and I find I haven't had to change it much for what I'm saying today. Change happens slowly in voting equipment and even now, with over eight months to go, it's too late to replace the equipment we'll use to vote this November 2018. My best advice is that we need *contingency planning*. In 2012, when Hurricane Sandy disrupted elections in several northeastern states, this was a big topic of discussion[14]. The National Association of Secretaries of State prepared a summary of relevant statutes in every state[15]. 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

---

[14] See, e.g., Kaplan, "Using Hurricane Sandy as a Lesson for Future Elections", *New York Times* (November 12, 2013) http://www.nytimes.com/2013/11/13/nyregion/lessons-from-hurricane-sandy-being-applied-to-election-planning.html

[15] 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

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 (NASED). The problem was that the money was allocated to the States before the EAC was up 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 errors[16], 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 EAC[17], 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. Such "risk limiting audits" are one of the best election practices available and should be adopted statewide.

[16] 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.

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

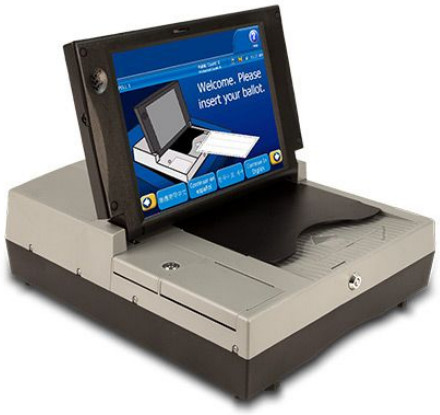

Fig. 1: ES&S DS200, precinct-based optical scanner with on-screen assistance features.

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)[18], as seen in Fig. 2, and the Travis County STAR-Vote (Secure, Transparent, Auditable, Reliable) system[19] 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 and allow for risk-limiting audits as well.

[18] http://vsap.lavote.net/
[19] http://traviscountyclerk.org/eclerk/Content.do?code=E.34

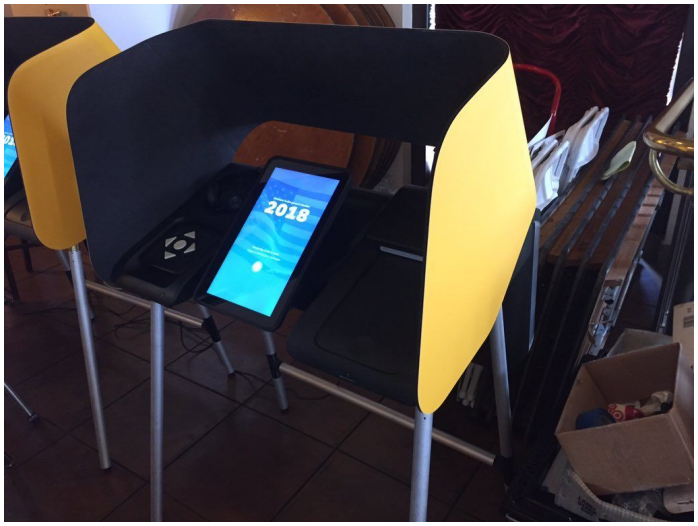

Fig. 2: Los Angeles VSAP prototype, with button-box, touch-screen, and printer.

Travis County ran a procurement process that ultimately failed to find a bidder for one of the essential components of the system. They're currently looking at other options, but I'll note that the design we came up with for Travis County would work just as well for the rest of the state, and the economies of scale that could come with a state-wide procurement would make a huge difference.

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 hours[20]. 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, Australia[21], and in Estonia[22], finding similar

[20] 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
[21] 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

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.[23]

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

---

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

[23] 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/

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.

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.

Recommendations

I have a number of specific policy recommendations that I believe can improve the security, reliability, and transparency of Texas voting systems and voter registration systems:

- Begin a process to retire and replace our aging, paperless, "direct recording electronic" (DRE) voting systems. Their security can no longer be guaranteed.
- Improve statewide standards to ensure that replacement equipment has better security than the outgoing DRE systems.
- The order matters: We need better standards *before* replacing our voting machines.

- Create statewide standards for managing back-end election data systems (from voter registration through vote tabulation and reporting), including expert teams that can assist counties in improving their cybersecurity posture.
- Consider centralizing the creation and management of tools for voter registration management, allowing for more intensive cybersecurity reviews.
- Consider centralizing the creation and management of voting systems, themselves. Texans should vote with state-of-the-art systems like Travis County's STAR-Vote design, representing a significant improvement in election security.
- Expand the responsibilities of the Texas Secretary of State's role in certifying voting systems to also include certifying voter registration and management systems.
- Standardize and promulgate election auditing procedures, including risk limiting audits that might occur during the "canvass" period (post-election / pre-certification) as well as after an election is complete. Such procedures can increase voter confidence that election outcomes are correct and can help counties discover and correct procedural mistakes that might have occurred.
- Ensure that the Texas Secretary of State's office is coordinating closely with the Department of Homeland Security to share and respond to threat information as it becomes available.

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, as in November 2016, 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.

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 20 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).