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?

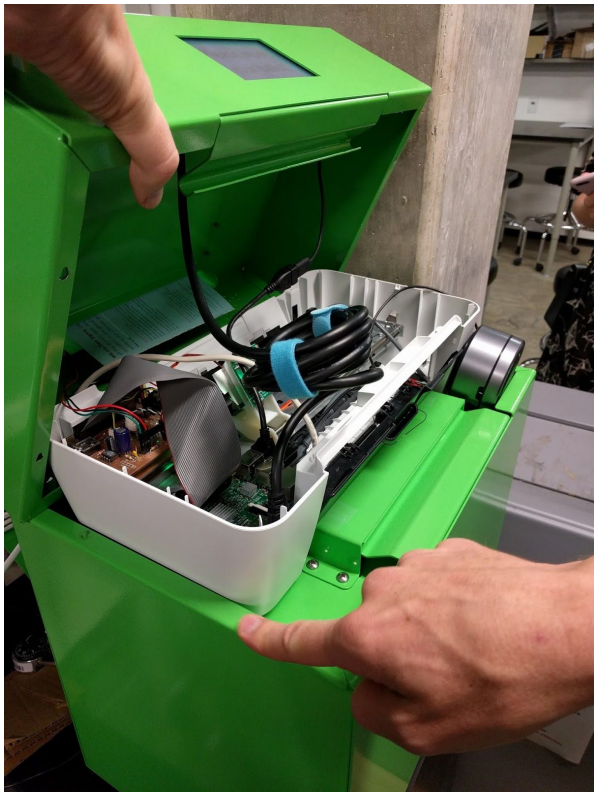
The National Science Foundation supports my own research in this area, as well as that of many of my colleagues, but there are no large efforts akin to DARPA's "grand challenges" being pursued at this time by any Federal agencies. The two most promising efforts, at the present time, are being pursued 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 voted[1]. 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).