THE CENTRE FOR
e-DEMOCRACY

Technology & Elections Policy Brief Series

Security Issues with Online Voting

Dr. Dan S. Wallach

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

http://www.cs.rice.edu/~dwallach/

FN Digital Democracy

McMaster University

Université d'Ottawa CĒPI Centre d'études en politiques internationales

University of Ottawa CIPS Centre for International Policy Studies

Social Sciences and Humanities Research Council of Canada

Conseil de recherches en sciences humaines du Canada

Canada

As a prelude to any discussion of online voting, it's important to understand the threats that an online voting system might face. We've learned that foreign nation-state actors, likely Russian, broke into the U.S. Democratic National Committee (DNC) computers and released a variety of documents[1]. We also have evidence of attacks against online voter registration databases in Arizona and and Illinois[2]. So far as we know, the attackers intend to manipulate the outcome of the U.S. Presidential election coming this November. 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[3]. 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[4] which I'll summarize for you here. While my blog posts are written largely from a U.S. perspective, they're still relevant to the situation in Canada. If a foreign nation-state adversary, like Russia, might wish to manipulate things in the United States, why not also Canada?

Consequently, **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.** The partisan impacts are easy to envision. You can selectively

[1] 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*

[2] Isik off, "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*. See also, 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*

[3] 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*

[4] *https://freedom-to-tinker.com/2016/08/03/election-security-as-a-national-security-issue/* and *https://freedom-to-tinker.com/2016/08/09/a-response-to-the-national-association-of-secretaries-of-state/*

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. US-CERT has published a list of security tips for such procedures[5]. The essential question to ask, for the U.S. or Canada, is what emergency procedures can be brought to bear if and when you might determine that your voter registration databases are corrupt. For example, can "provisional" mechanisms, meant to allow voters to cast a ballot while their status is unclear, scale to support millions of disenfranchised voters? And if not, then what alternative?

Can our adversaries get malware into our voting machines, themselves? Military organizations typically protect their 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 nonetheless[6]. 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. *To the extent that Canadian voters are*

5 https://www.us-cert.gov/ncas/tips/ST16-001

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

using paperless electronic voting systems, including Internet voting systems, this is a significant issue.

Does an adversary need to attack everywhere? Our adversaries understand how our political systems works. They can focus their efforts on specific cities or provinces 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.

What can we do in the short-term? My best short-term 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 discussion[7]. The U.S. National Association of Secretaries of State prepared a summary of relevant statutes in every state[8]. 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. In the U.S., state and local election officials can

[7] 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*

[8] *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*

request assistance from the Federal government in this process as well. If the Canadian federal government doesn't already offer similar services, they should.

How do we make sure we won't face these risks in subsequent elections? Or, stated another way, what sorts of election systems make sense in light of the threats posed by nation-state adversaries, never mind limited budgets with which to procure those election systems? I see two options:

Next-generation optical scan systems: The big elections equipment vendors are all now selling "precinctbased 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[9], 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[10], 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.

Nextgeneration 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)[11], as seen in Fig. 2, and the Travis County STAR Vote

[9] 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.

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

[11] http://vsap.lavote.net

(Secure, Transparent, Auditable, Reliable) system[12] 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.

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

I'd next like to address the risks of Internet 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[13]. They were able to

[12] http://traviscountyclerk.org/eclerk/Content.do?code=E.34

[13] 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

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[14], and in Estonia[15], 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.[16]

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 secretballot 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

[14] 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*

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

[16] Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", Forbes (Jan. 2016), *http://www.forbes.com/forbes/welcome/?/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/&to*

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 government bodies to standardize these things, making it easier for a remote voter to cast a private vote in a controlled polling location.

Conclusions

As former U.S. Secretary of Defense 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 America's systems for voter registration, casting, and tabulation. None of them are ready to rebuff attacks from our nationstate 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. Canada can and should take similarly pragmatic steps. Canada should not make the mistake of growing its use of Internet voting systems, since that only increases its vulnerabilities to foreign nation-state attackers, and other adversaries.

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).