How Close Are We to Internet Voting?

You can do basically anything online. From booking a flight to securely transmitting medical records to your doctor, from buying groceries to managing your bank account, the web supports all sorts of complex transactions. But one common task has firmly resisted the lure of online convenience: voting.

At least mostly. There is actually some online voting already happening in very limited ways. At least 32 states and the District of Columbia will allow military or overseas voters to return absentee ballots via email, fax or an Internet portal, in effect offering a form of remote electronic voting to some segment of the population. But for the majority of voters, a trip to a polling place will be necessary to cast a vote in this year's election.

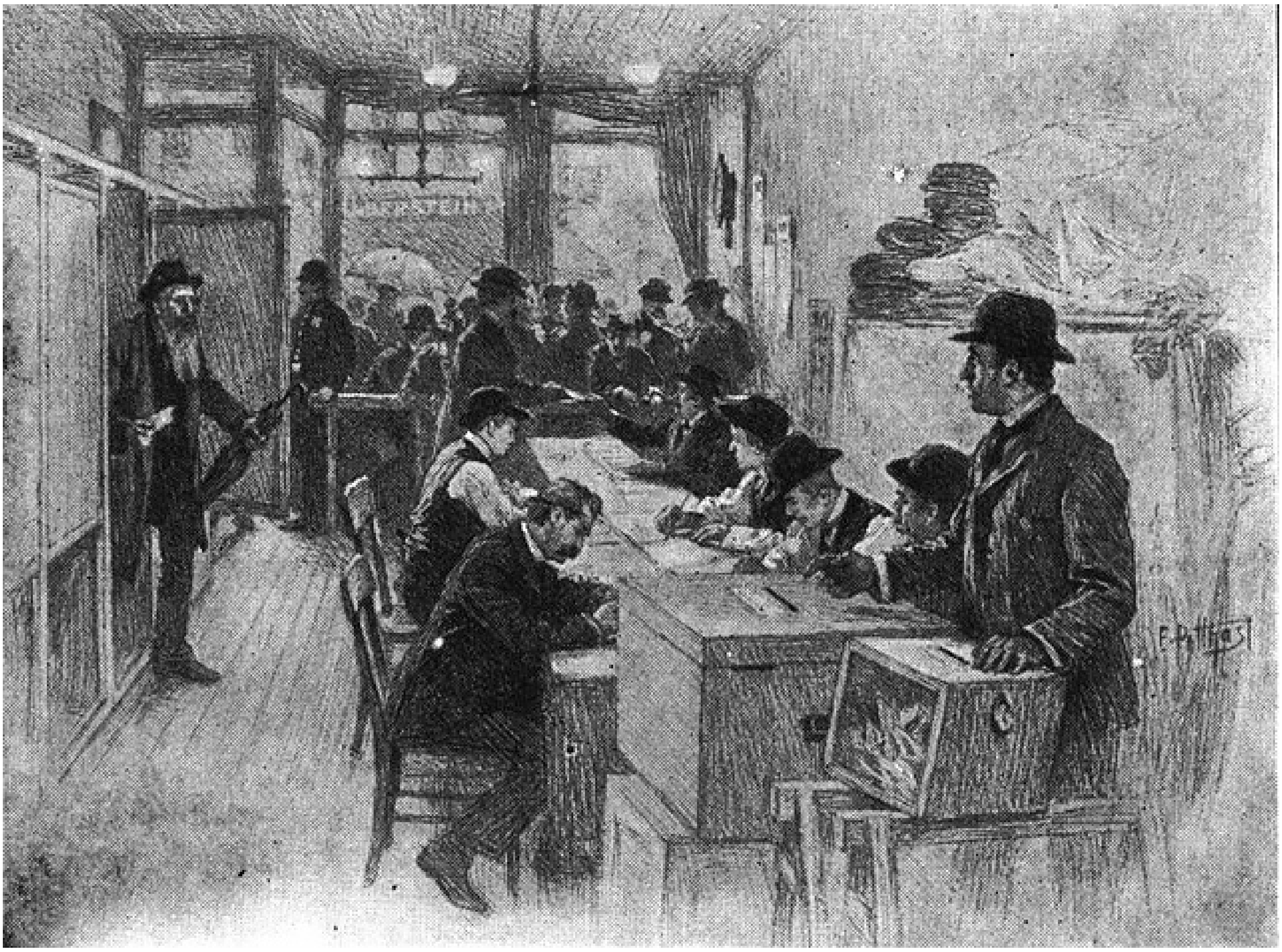
Why is that? Surely, if engineers can figure out how to safeguard your medical records or transfer large sums of money over the Internet, beaming a vote from your living room should be a piece of cake. That's a popular refrain among proponents of Internet voting systems, and on the surface, it makes sense. If security-obsessed industries like banking and medicine have embraced the Internet, why is voting still stuck in the relative dark ages? As with most things, the reality is a bit more complicated.

According to VerifiedVoting.org [1], a non-profit organization dedicated to ensuring the "accuracy, integrity and verifiability" of elections in a digital age, all voting systems should have a few key components. First, there needs to be a fully auditable, preferably voter-verifiable paper trail that maintains the integrity of the secret ballot. Second, voting systems need to have in place strong mechanisms to prevent any undetected changes to votes. Third, systems should not be easily subject to wide-scale service disruptions. Indeed, the Help America Vote Act [2] (HAVA), passed in 2002 as a response to the Florida recount debacle of 2000, requires some of these provisions under the law.

From a strictly engineering standpoint, none of those problems seem impossible to overcome. So why did VerifiedVoting.org board member and Lawrence Livermore National Laboratory computer security expert David Jefferson tell attendees [3] at the RSA Security Conference in March that the very concept of Internet elections is “unfixably broken?”

Let’s dig into each of VerifiedVoting.org’s requirements for a voting system and how they might be achieved via the Internet.

Voting systems must have an auditable paper trail



[4]

Both critics and proponents of online voting agree that it is important for all votes in an election to be counted as cast. Where they disagree is how best to make that happen. The voting system standards laid out in the Help America Vote Act require that all voting systems “produce a record with an audit capacity for such system,” or in other words, votes can be recounted for verification purposes.

For traditional voting systems, that usually means votes are cast by some method that involves making a permanent mark on paper, like punching a hole through a card or marking a box with a pen, and then dropping those ballots into a box to be manually counted, or feeding them into some sort of electronic counting machine. Electronic systems used at polling places often create a printed receipt that details the vote you just cast. Online voting critics argue that this paper record is the most reliable way to ensure votes can be verified in the face of a discrepancy or too-close-for-comfort results.

Pamela Smith, president of VerifiedVoting.org, says that audit trails should create an “indelible record, not something that’s ephemeral, like bits and bytes.”

And some in the government seem to agree. A 2011 study [5] from the National Institute for Standards and Technologies concluded that online voting systems weren’t ready for prime time, in part because “Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems.”

Of course, Internet voting systems are already being used in elections of consequence, and the people who make them argue that their electronic ballot systems are actually more secure and more reliable than the paper versions in use today.

“The premise that a piece of paper is immutable and therefore the best answer for proving that something was what it was intended to be doesn’t make sense to me,” says Lori Steele, CEO of Everyone Counts [6], a vendor of online and electronic voting systems that have already been used for elections in cities and states all over the U.S. According to Steele, her company’s software delivers a more reliable audit trail because it is more secure than paper, and because electronic systems can create multiple, independent copies of voting records that can be checked against one another. That sort of redundancy doesn’t exist in today’s paper systems, where you fill out one piece of paper to rely on in the event of a recount.

“Just because someone sees a piece of paper going into a cardboard box, doesn’t mean that that piece of paper was what was delivered in the end and counted,” argues Steele, who alludes to horror stories of paper ballots lost [7] or stolen [8] and never counted.

And what about the privacy requirements? Most democratic governments, including that of the U.S., are elected via a secret ballot in order to stop coercion, intimidation or simple vote selling. Currently, some states that allow overseas voters to return ballots by electronic means, like email or fax, require them to sign an affidavit that acknowledges the secrecy of their vote may be impossible to protect. VerifiedVoting.org says that creating a reliable audit trail while maintaining the secret ballot is an unsolved problem. Steele says her system already meets those requirements.

It really comes down to this: Can you trust an electronic record? Your mileage may vary.

Voting systems must have mechanisms in place for detecting changes to votes

Online voting critics have horror stories to share, too. Smith recounted what happened in 2004 in Carteret County, N.C., when an unanticipated memory limitation on an electronic voting machine caused the system to simply stop counting votes. About 4,500 were lost before anyone noticed. Or the 2010 D.C. pilot program test [9], in which a team of computer security students from the University of Michigan were able to hack into the system and change not only the results, but the actual choices displayed on screen. (Steele says that one was the result of sloppy code on the part of the vendor of that particular system.)

Even though Steele claims that Everyone Counts' software uses highly complex, military-grade encryption that is nearly unhackable, she concedes that in computer security you can never say never. "Technology changes fast. It's important that we maintain our state-of-the-art standards in both security and accessibility," she says.

That's a big concern for critics, who note that even if you can assume an online system is no more secure than our current standards, they exponentially increase the attack surface. It's much easier to hack into a broadly used system and alter thousands of votes than it is to counterfeit thousands of paper ballots.

If a nightmare scenario were to manifest, and a voting system was hacked and not detected, we may never know, according to Jefferson. That's the main difference between banking and voting, he said at the RSA conference. Because of the privacy requirements, there's no list of voter decisions that allows you to check and say, "Yep, my vote was recorded correctly." According to Jefferson, it's more likely that the wrong person takes office and life goes on with no one the wiser.

That's a troubling scenario, but it seems to ignore that the same methods used today to uncover discrepancies in the vote — like exit polling and automatic recounts — could still be employed. As long as that audit record exists, any election should be verifiable.

Voting systems must not be subject to wide-scale service disruptions

Perhaps the most serious potential issue for online voting systems is the threat of a distributed denial of service attack. While our current network of polling places leaves thousands of voters disenfranchised each election cycle, because of long lines, poorly publicized poll location changes, the inability to travel or misinformation — a wide-scale DDoS attack could theoretically disenfranchise large swaths of the voting public.

It's not that hard to imagine a large-scale attack, or even something more mundane like a power outage, rendering an entire election network unreachable by voters. In June 2012, a power outage caused a service disruption to Amazon Web Services [10], bringing down popular websites like Instagram [11] and Netflix [12]. A similar outage [13] in 2011 affected other web heavyweights.

Then in September 2012, an attack [14] on the servers of domain registrar and web host GoDaddy [15] impacted thousands of web sites. That attack was allegedly perpetrated by someone connected to often-politically motivated hackivist group Anonymous [16] (though GoDaddy refutes this [17]). Is it such a stretch to imagine that a group like Anonymous could someday want to impact a major election via DDoS attacks on the voting servers?

Steele admits that DDoS attacks are “absolutely a problem; a more real problem than others,” but also assures that her company takes steps to mitigate the threat. One unique condition of online voting that acts in her favor is that Internet-based elections can be held for longer than a single day, and usually they are. Steele said that most online voting takes place over the course of a few weeks.

“So the chances of having a denial of service attack have an impact are also slim,” she says, “because it would have to be a very long, extended denial of service attack over multiple days that also touched each of the hosting facilities that was hosting the election.”

Also working in her favor is the fact that elections are a multi-billion dollar business, and the free market is very much at play. There are thousands of election jurisdictions [18] in the U.S. and they don’t all use the same platform or vendor. So while you might have a trade-off when it comes to usability or auditability between vendors, all those different competing systems that connect to different hosting facilities actually act as an extra layer of security.

That panoply of different systems also protects against the computer systems of individual voters becoming targets. As many as 48% of computers [19] in the United States may already be infected with malware. As is often pointed out by security experts, the weakest link in any online system is the home computer.

Malware installed on a computer used to vote could, for example, make a user think he was casting a ballot for one candidate, but actually send a completely different vote to the server, or send no vote at all. If a piece of malware replaced an official voting app on your device with a dummy version or redirected you to an unofficial version of an official website, and your vote was never recorded, would anyone ever know? Probably not. Or at least, not until it was too late to recast your vote.

Still, Steele rejects this as a valid concern. Online voting doesn’t necessarily mean via a web browser on a PC — it can also mean through an app on an iPad [20] or a smartphone. With more and more people owning multiple devices, it would be very difficult for anyone to effectively attack the vote via malware.

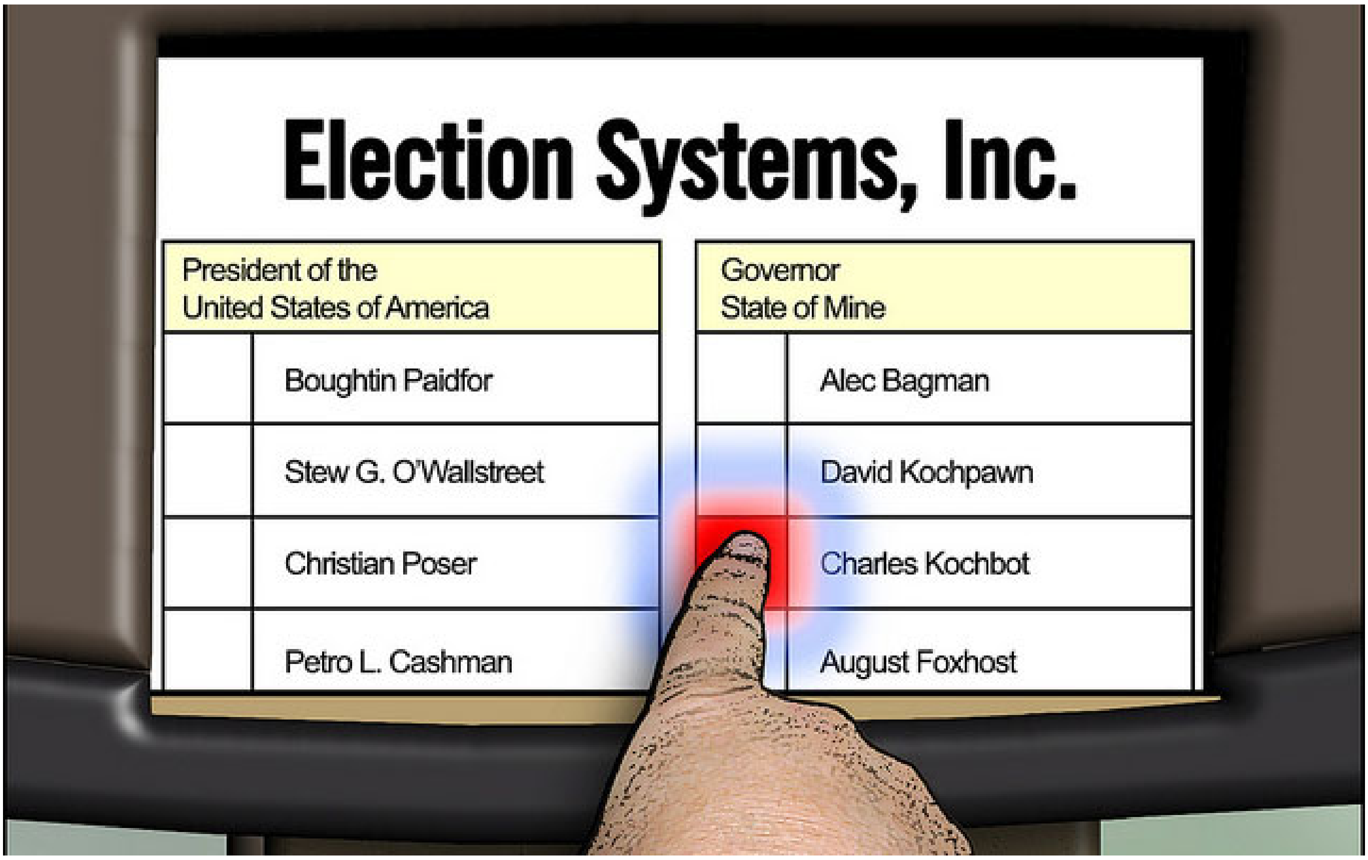
“To be able to infect all of [your] devices for everybody in America to make sure that you can actually impact the election is a lot harder than signing up as a poll worker and throwing ballot boxes in the river,” argues Steele, who indicated that Everyone Counts also employs detection methods to check computers for dangerous malware before letting a constituent cast her vote.

The Flame virus [21] discovered earlier this year indicates that nothing is completely safe. That virus was in the wild for two years before it was detected by security experts, stealing information like Skype conversations and keystrokes without detection. Flame reportedly even had the ability to self-destruct [22] and erase itself from infected computers.

Could a Flame-like virus be infecting online voting systems without anyone knowing? While Steele probably wouldn't admit it, Flame, and other recently discovered viruses like Stuxnet and Gauss, indicate that malware creators are often one step ahead of the security experts chasing them. As John Naughton wrote [23] in *The Observer*, "The PC security business … suffers from one structural problem: its products are, by definition, *reactive*."

That might be a serious issue when you're dealing with something that has gravely important and wide-reaching consequences like a national election.

Internet voting is coming



[24]

It would be naive to think that Internet voting isn't coming. Indeed, as Steele was quick to point out, online voting is already here, and will be used by many in the 2012 presidential election. Proponents of online voting point to a number of reasons to embrace the technology. Online voting systems are by their nature more accessible (another requirement of HAVA); they make it difficult to suppress votes by dubious methods like redistricting; and there is some evidence that voter turnout increases when online voting options are presented (though this is up for debate [25]).

Military and overseas voters could especially benefit from the ease of use and accessibility of online ballots, say representatives from the Operation Bravo Foundation [26], an organization whose mission is to increase success for people who cast their vote under the Uniformed and Overseas Citizens Absentee Voting Act [27] (UOCAVA). According to Operation Bravo president Pat Hollarn, success is measured by voter satisfaction in receiving a blank ballot on time and returning it with an assurance that it will arrive back in the U.S. on time to be properly counted. However, the chance for success is much lower for UOCAVA voters than among stateside absentees. She cites reasons like postal delays caused by extreme remoteness, address changes (ballots aren't supposed to be forwarded), last-minute military deployment and issues with ballots being handed off to foreign postal services.

"People are extremely comfortable with what they're familiar with," says Steele, explaining why online voting is not yet more widespread. It's easy to imagine a time in the near future when the majority of registered voters are people who grew up completely in today's digitally connected world. At some point, online voting may become necessary for widespread civic participation.

That's not a good enough reason for critics to put their trust in Internet-based systems. "Fourteen-year-old kids want to drive fast and not wear seat belts, but we don't let them. It's not an option," says Smith. "And the reason it's not an option is not just because we're safeguarding them, but we're safeguarding the rest of us, too."

Smith is right that elections are important enough that decisions about voting systems should not be based solely on the whims of the populace. But the writing on the wall seems clear: Widespread online elections will be a reality in the near future. So rather than fight it, a more productive tack would be to make sure that when the day arrives that anyone in America can cast his vote online, it's accomplished with the most secure and foolproof systems imaginable.

As Steele points out, employing a variety of elections systems is a boon for security, but it also means that not every vote may have the same level of auditability. That's why there should be national standards in place and vendors should be forced to share best practices with one another. It should also be mandatory that vendors make their code available for peer review (something Everyone Counts does voluntarily). HAVA required that the United States Election Assistance Commission set up guidelines for verification of voting systems [28], but many critics and proponents of online voting agreed that the standards lack stringency, especially when it comes to over-the-Internet voting — and the guidelines haven't been updated since 2005, though a second draft was submitted in 2009. Further, federal certification of electronic voting systems is currently voluntary and only nine states require testing to federal standards [29].

The bottom line is that elections need to be trustworthy. "How many votes can we afford to lose?" Smith asks. "The answer should be zero, or as close to that as we can get."

That's something everyone can agree on.

Read More [30]

October 03, 2012

Source URL (retrieved on *05/20/2013 - 11:43pm*):
http://www.wirelessdesignmag.com/news/2012/10/how-close-are-we-internet-voting?qt-blogs=0

Links:
[1] http://www.verifiedvoting.org/
[2] http://www.eac.gov/about_the_eac/help_america_vote_act.aspx
[3] http://technorati.com/politics/article/why-internet-based-voting-is-unfixably/
[4] http://9.mshcdn.com/wp-content/uploads/2012/10/voting-paper-trail.jpg
[5] http://www.nist.gov/itl/vote/uocava.cfm
[6] http://everyonecounts.com/
[7] http://www.freerepublic.com/focus/f-news/2622073/posts
[8] http://www.sfgate.com/bayarea/article/Stolen-ballots-found-all-wet-in-the-Marina-3167539.php
[9] http://online.wsj.com/article/SB1000087239639044450850457759528067487018 6.html
[10] http://mashable.com/2012/06/30/instagram-down-power-heat-wave/
[11] http://www.mashable.com/follow/topics/instagram/
[12] http://www.mashable.com/follow/topics/netflix/
[13] http://mashable.com/2011/04/21/amazon-aws-server-problems/
[14] http://mashable.com/2012/09/10/godaddy-down/
[15] http://www.mashable.com/follow/topics/godaddy/
[16] http://mashable.com/follow/topics/anonymous
[17] http://mashable.com/2012/09/11/godaddy-denies-hack/
[18] http://www.eac.gov/research/election_administration_and_voting_survey.aspx
[19] http://www.zdnet.com/blog/security/report-48-of-22-million-scanned-computers-infected-with-malware/5365
[20] http://www.mashable.com/follow/topics/ipad
[21] http://mashable.com/2012/05/28/flame-cyber-weapon-security/
[22] http://mashable.com/2012/06/08/flame-self-destruct/
[23] http://www.guardian.co.uk/technology/2012/jun/17/flame-virus-online-security
[24] http://9.mshcdn.com/wp-content/uploads/2012/10/electronic-voting.jpg
[25] http://www.theglobeandmail.com/news/british-columbia/bc-looks-to-e-voting-to-increase-turnout/article4472692/
[26] http://www.operationbravo.org/
[27] http://en.wikipedia.org/wiki/Uniformed_and_Overseas_Citizens_Absentee_Voting_Act
[28] http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx
[29] http://www.eac.gov/testing_and_certification/testing_and_certification_program.aspx
[30] http://mashable.com/2012/10/02/internet-voting/