David Jefferson
Computer Scientist, Lawrence Livermore National Laboratory[1]
Board of Directors, Verified Voting Foundation
Board of Directors, California Voter Foundation
d_jefferson@yahoo.com

If I can shop and bank online, why can't I vote online?[2]

1. Introduction

Many people look forward to the introduction of some form of Internet voting in public elections. They like the idea of voting online, all electronically, from their own personal computers or mobile devices, whenever and from wherever they wish. Proponents argue that Internet voting would offer greater speed and convenience, particularly for overseas and military voters, and might offer new possibilities for disabled voters as well. Some believe that voter participation would increase, particularly among young people because of their familiarity and comfort with online media. The idea of convenient voting any time from any computer or mobile device has wide appeal.

However, computer and network security experts are virtually unanimous in agreement that online voting is an exceedingly dangerous threat to the integrity of U.S. elections. There is no known way to guarantee that the security, privacy, and transparency requirements for online elections can all be met with any practical technology, not now and not in the foreseeable future. Anyone from a disaffected misfit individual to apolitical partisan to a foreign national intelligence agency can remotely attack an online election, modifying or filtering ballots in ways that are undetectable and uncorrectable, or just disrupting the election and creating havoc. There are a host attack methods that can be used singly or in combination. In the cyber security world today almost all of the advantages are with attackers, and any of these attacks can result in the wrong persons being elected, or initiatives wrongly passed or rejected.

Nonetheless, enthusiasts point to the fact that millions of people regularly bank and shop online every day without apparent problems. They are often convinced that online voting can be similarly easy by the fact that a voting transaction superficially resembles an ecommerce transaction. You connect your browser to the appropriate site, authenticate yourself, make your choices with touches or a mouse click, then click on a final confirmation button, and you are done! And since all of the potential attacks on online voting alluded to above apply equally to online shopping and banking,

---

[1] *Analyses and views stated herein are drawn from my expertise as a computer scientist working on national security applications and are my own. They are not to be ascribed to my employer, Lawrence Livermore National Laboratory, which takes no position on these issues.*

and they seem secure enough, what is the difference? It is thus natural to ask, *"If it is safe to do my banking and shopping online, why can't I vote online?"*

This is a very fair question, and it deserves a careful answer because the reasons are not obvious. Unfortunately it requires substantial development to explain fully. But briefly, the answer is in two-parts:

1. It is *not* actually safe to conduct ecommerce transactions online. It is in fact very risky, and more so every day. Essentially all the same risks, and then some, apply to online voting.
2. The security, privacy, transparency and other requirements for voting are structurally different from, and much more stringent than, those for ecommerce transactions. Even if ecommerce transactions *were* safe, the security technology underpinning them do not suffice for voting. Voting security and privacy requirements are unique in ways that have no analog in the ecommerce world.

The rest of this essay expands upon these two points.

2. Ecommerce transactions are not, in fact, "safe"

Why do security experts say that ecommerce transactions are not safe when millions of people do them every day, mostly without problems? The question needs to be refined: "Safe for whom?" and "What degree of safety is required"?

2.1 Online threats

Ecommerce transactions may be relatively safe for consumers, but they certainly are not safe for financial institutions or merchants. Banks, credit card companies, and online merchants lose billions of dollars a year in online transaction fraud[3] despite huge investments in fraud prevention and recovery. Consumers have the illusion that ecommerce transactions are safe because merchants and banks don't hold them financially responsible for fraudulent transactions when they are innocent victims. Instead businesses absorb and redistribute the losses silently, passing them on in the invisible forms of higher prices, fees, and interest rates. Businesses know that if consumers had to accept online losses personally, most online commerce would collapse, so they routinely hide the losses. It is a sound business strategy.

But ecommerce fraud is very real, and many fraud techniques that are directly applicable to online voting. A common pattern starts with theft of *credentials*, e.g. names, account numbers, credit card numbers, passwords, or answers to personal challenge questions. The theft can be initiated through phishing scams, drive-by malware installation, key loggers, data stolen from hacking into major commercial establishments, or other means, and such tricks can just as easily be used to steal online voting credentials.

Recently a malware family named Zeus has been in the news.[4] It installs malware on PCs that is specifically designed to wait until you connect to your bank and then it steals your bank account number and password as you type it into your browser. The Zeus botmasters use those credentials to transfer money out of your accounts and to fake your online financial statements to hide the theft from you for as long as possible.

It makes no difference that you have a "secure" connection to your banking site because the malware operates inside your own computer and it can see and modify everything you type while it is still in the clear, before it is encrypted for secure transmission. There are now illicit businesses that

---

[3] See http://www.mcafee.com/us/resources/reports/rp-financial-fraud-int-banking.pdf, p. 4

[4] See http://en.wikipedia.org/wiki/Zeus_(trojan_horse)

help people set up Zeus botnets, or rent time on one already created.[5] Unfortunately most people are completely unaware of such online threats.

Zeus exemplifies what could easily happen if online voting becomes widespread. Eventually someone, perhaps a partisan political operative or a foreign intelligence agency, will deploy a similar botnet to infect perhaps hundreds of thousands of voters' computers and steal their credentials or modify their votes invisibly, right as they are being transmitted. Again, having a "secure" connection to the remote election server will make no difference at all. There is generally no effective way to prevent such an attack, and no effective recovery. Banks, online merchants, and high tech companies that do business online have huge security budgets to defend themselves against cyber attacks, and even so they are frequently victimized. If these organizations with such great expertise and capability in computer and network security can be successfully attacked, then no voting system vendor or local election administration has any realistic chance of successfully defending against similar threats.

The cost to an attacker of conducting a remote online attack has declined drastically over the last few years as various programming templates, libraries, and toolkits for malware production have become widely available. One recent study demonstrated that it was possible to duplicate even very sophisticated attack vectors like Stuxnet, the malware that did great damage to Iranian nuclear centrifuge facilities, in about two months time for under $20,000.[6] We are now in a very different threat environment than we were even a few years ago.

2.2 Degrees of safety required for ecommerce and voting

What level of security is sufficient to protect elections? The scale of fraud that ecommerce and electoral systems can tolerate are very different. In the ecommerce world if one out of every thousand transactions is lost or fraudulent it is not really a vital concern. Banks, merchants and purchasers routinely deal with online revenue losses over 10 times higher than that[7], and have many tools to deal with the loss. As unjust and frustrating as it may be, no catastrophic consequence ensues from a small ecommerce fraud rate.

But in the voting world we are all familiar with the cases where, within about one decade, a senator, a governor, and a president were all elected by margins much smaller than one vote in a thousand. Election outcomes are thus *very sensitive to small errors or frauds* in a way that ecommerce systems simply are not. Small changes in vote totals sometimes have national or global consequences. Election security is thus a matter of *national security*, and the security standards have to be designed to reliably prevent, detect, and correct even very small problems and attacks. That level of security and reliability is not needed and not cost effective for ecommerce systems.

3. Voting security, privacy, and transparency requirements are structurally different from those for ecommerce transactions

The second point of our argument is that the security, secrecy, and transparency requirements for online voting transactions are structurally very different from, and generally much stricter than, those for ecommerce transactions. The security mechanisms that make ecommerce transactions relatively safe (for consumers at least) are not sufficient to guarantee the safety of online voting.

---

[5] See http://threatpost.com/en_us/blogs/new-service-helps-attackers-get-zeus-botnet-ground-011011

[6] See http://hosted.ap.org/dynamic/stories/U/US_TEC_HACKING_CONTROL_SYSTEMS?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2011-10-23-08-23-54

[7] See http://www.mcafee.com/us/resources/reports/rp-financial-fraud-int-banking.pdf , p. 4

3.1 Auditability, detectability and correctability of problems

The first major distinction is that we can at least eventually *detect* ecommerce errors and fraud, but we may never know about online election fraud.[8] In the ecommerce world problems are reliably detected because of such practices as receipts, double entry bookkeeping, and financial audit records kept by both sides of every major transaction. Even in the absence of those practices it will be detected eventually when some transaction that should succeed unexpectedly fails because an account is out of money.

But in most kinds of online elections there is nothing that corresponds to receipts, double entry bookkeeping, or meaningful audit trail information. Security experts routinely call for an independent, end-to-end audit trail that can be used to verify that the electronic ballots received by election officials are identical to those the voters sent, and that none were forged, lost, or modified in transit. But the only reliable way to accomplish this with current technology is for voters to send verified paper copies of their voted ballots back to their local election officials, and for the officials to use those copies in a formal risk limiting audit procedure.[9] That would actually solve most of the security problems associated with online voting (though not the privacy problems). However, most advocates of Internet voting oppose such a paper-based audit requirement because the additional burden on voters to mail back paper copies of their ballots is essentially equivalent to sending an ordinary paper absentee ballot, which is what most of them wish to avoid. Yet without a meaningful end-to-end audit trail a well-constructed attack may lead to the attackers' choice of candidates being elected and *there may well be no way to know that anything happened at all.*

Even if there is suspicion of a problem there will be no way to prove or disprove it. Because of ballot secrecy, even if there were strong evidence that *particular* persons cast illegal ballots, or their ballots were tampered with, officials cannot know *which* ballots to remove from the count. Hence, fraudulent online voting will often be *undetectable,* and almost certainly *uncorrectable* even if detected.

3.2 Structural differences between the security requirements for voting and ecommerce transactions

There are several ways in which the security requirements for voting are strictly stronger than those for financial transactions. Eligibility checking is one. In the ecommerce world essentially anyone, including criminals, non-citizens, and minors, is allowed to buy and sell online. Non-human entities, e.g. corporations, government agencies, and estates, are free to engage in ecommerce transactions as well. And there are usually no residency requirements for ecommerce transactions. But those factors all play a role in determining eligibility to vote, and are verified (in principle at least) at the time of voter registration. An online voting system thus must determine that the voter is legally registered in the jurisdiction in which he or she is casting a vote.

Then there is the issue of proxy transactions. In the ecommerce world you can freely authorize someone else to act as your agent for purchases or funds transfers simply by giving them your credit card number, security code, and password. For larger transactions you can accomplish the same thing by setting up a joint bank account, signing a contract, appointing a trustee or guardian, granting power of attorney, etc. But in the voting world you are *never* permitted to transfer your right to vote to anyone else, at least not in the U.S. No one is legally allowed to act as your proxy to vote for you on your behalf — not even your spouse or guardian or caregiver, and not even with your written permission.

---

[8] See http://servesecurityreport.org/paper.pdf

[9] For papers on audit procedures for elections a good place to start is http://statistics.berkeley.edu/~stark/Vote/#papers

The prohibition of double voting is a third election security requirement that has no analog in the ecommerce world. You are free to engage in as many ecommerce transactions as you please, but you may cast only one ballot per election. Enforcement of the double vote prohibition is actually somewhat complex because it has to cover not just voting a second time online, but also voting a second time by paper absentee ballot or in person at the polls. And it should also prevent you from casting two votes in different jurisdictions in the same election, though that is difficult to enforce.

3.3 Authentication and identity determination

Because of the need for eligibility checking, proxy vote prevention, and double vote prevention an online voting system must *verify the actual identity of voters*. We need a strong identity verification mechanism because if an attacker can figure out how to cast one illegal vote online through a weakness in the identity verification, then he can probably automate that attack to cast thousands of phony votes. But reliably verifying the actual identity of a potential voter remotely through the Internet is a difficult and unsolved problem in the U.S. The U.S. does not issue national identity cards with private keys embedded in them. Nor do election jurisdictions keep a database of faces, fingerprints, or other biometric data (except for ink signatures) about registered voters, and even if they did computers today are not equipped to capture and transmit them securely. It is not sufficient for the voter to just present a password or to answer to a challenge question (e.g. "What city were you born in?"). Any such data might be given away, guessed, cracked, stolen, or sold, and enables *automated* online buying and selling or stealing of such voting credentials.

In most states voters prove their eligibility to vote when they register and provide an ink signature sample for use later use. Voters prove their identity again when they vote, either at the polls or via paper absentee ballot, by duplicating that ink signature on record in the registration database. Some states are now going even further and requiring voters to provide photo ID documents at the time of voting. But we cannot get a wet ink signature from a voter through the Internet to compare against the registration records, nor can the voter present his or her face along with a matching photo ID or passport. *As of now there is no reliable infrastructure in place to verify over the Internet the actual identity of a person sitting at a PC or holding a mobile device*.

In contrast, for an ecommerce transaction we only have to verify that the person doing the transaction is *reasonably certain to be authorized to use the financial account he is charging to*, which is a much lower requirement. There is no strong identification requirement for ecommerce transactions. All that is really required for an online transfer of funds out of your bank account is the name, account number, and password associated with the account. *There is no strong verification of the actual identity of the person doing the transaction*. Or when you sign up for an ecommerce account, e.g. at amazon.com, they ask for your name and address, but they do not ask for a picture, or an ink signature, or your driver's license, or passport, or other strong proof of identity. They never check those, and have no way to do so. To make a purchase from Amazon all that is *really* required is reasonable evidence that you are in possession of some (any!) valid credit card. You demonstrate that by giving the name on the card, the account number, security code, expiration date, and password, but you do not need to present and strong ID. If the transaction goes through, the purchase is complete. Online merchants do like to know who their customers are for marketing purposes, but when it comes down to it they will generally sell to anyone who can type in numbers and passwords for a valid account and valid credit card. It is good business practice. If the credit card turns out later to have been stolen, the problem will be sorted out after the fact.

3.4 Privacy and secrecy requirements

The privacy requirements for ecommerce and for voting transactions are fundamentally different. An ecommerce transaction is generally *symmetric* between buyer and seller, with both parties in theory fully aware of all the details of what is being bought and sold, for what price, with what warranties, and who has what rights to void the transaction, etc. For larger transactions there is usually an exchange of official paper, e.g. signed contracts or receipts, with all the relevant

transaction details so that in case of a dispute either the buyer or seller can *prove* to a third party (e.g. a court) exactly what the transaction was supposed to be so the dispute can be resolved.

But it is not the same with voting transactions. The voter of course knows the details of his votes, but election officials must not. Officials know the names of those who voted and the contents of the cast ballots, but they are never supposed to know exactly who cast which ballot. This is a strong requirement for partial blindness on the part of one side in the transaction that has no analog in the ecommerce world. Furthermore, although each voter knows how he personally voted and is free to tell anyone, he is not allowed to have any *proof* of how he voted that could convince a third party. This inability to prove how you voted is the most powerful protection we have against the threat of vote selling and vote coercion, and is a requirement unique to voting. I know of no other security situation in which people are completely free to *disclose* a fact that they know (how they voted), but are not permitted to have any *proof* of that fact that can convince someone else that they are telling the truth.

3.5 Irreversibility and risk management

Vote fraud is much less manageable than ecommerce fraud. There is no election analog to the natural business practice of "spreading the cost" or "spreading the risk". There is no "insurance" that one can buy to cover those losses. There is just no way at all to compensate for damage done by fraud to an election.

The unusual vote privacy rules have strong risk management consequences. As noted earlier, if for some reason officials learn after the fact that a particular person has succeeded in casting an illegal ballot there is no way to find it to remove it from the count. In the U.S. and most other countries once a voting transaction is complete it cannot be undone even in principle, so a voting transaction is *irreversible*.

In the ecommerce world, however, we go to some lengths to make sure most transactions are reversible. Merchandise can be returned, money can be refunded in whole or in part, records can be corrected. For that reason people feel free to take prudent risks with online financial transactions based on the reputation of the merchant or the credit history of the buyer. But there is no reversibility of voting transactions, and no concept of "reputation" or "credit worthiness" in the election world to help manage risk.

These differing vulnerabilities to failures and fraud lead to very different security approaches in online transaction software. For election security there is a very strong imperative for *up front, absolute multilayered prevention of errors and fraud*. For ecommerce there is usually much reduced need for strong security barriers up front because problems can usually be corrected later and those that cannot can be absorbed.

3.6 Transparency requirements

The flip side of privacy is *openness* or *transparency*, and once again, the requirements are completely different for ecommerce and for online voting. In the ecommerce world a person buying something online is entitled to know everything about his particular transaction, but nothing about other people's transactions. A buyer is not entitled to know how many other transactions there are, what the merchant's revenues or profits are, who else the merchant sells to, or what price others pay for the same goods or services, and he has no right to audit the books of the merchant he is dealing with.

In the voting world, however, most of this is reversed. Complete election information is (or should be) open to all. Election officials report not just the names of the winners, but also exactly how many votes were cast and how many each candidate received down to the precinct level. The list of exactly who voted is also usually public, and in some jurisdictions so are the original ballot images. In principle *all* information bearing on the outcome of an election that does not

compromise vote privacy is (or should be) public. Candidates, parties, and the public are entitled to participate in open audits, challenges, and recounts so that everyone, especially losing candidates, can be satisfied that the election was conducted according to law and the votes were counted accurately. Election officials are thus accountable to candidates and to the public for the integrity of every relevant detail of an election, whereas merchants are usually accountable only to buyers, and then only for each buyer's own transactions.

3.7 Fraud motivation patterns and national security

Finally we must take notice of the fact of life that the motivations for fraud are profoundly different in the commercial and electoral worlds. In an ecommerce situation all transactions are essentially independent. A buyer has no particular incentive to spoil or tamper with another buyer's online purchase since two buyers rarely have conflicting interests. In any case the problem would almost certainly be detected and corrected. And it is hard to imagine a motive for another nation to bother messing with many Americans' ecommerce transactions when, if it is inclined to some kind of cyber attack, there are so many other more immediately damaging targets.

But the situation is completely different with voting. There is a powerful partisan incentive to block or change other people's votes, especially if it can be done without detection. The motivation to *automate* that process to affect thousands of online votes is that much greater. Such attacks can be done for tens of thousands of dollars or less, while the monetary value of changing the outcome of an election can be hundreds of millions or billions of dollars or more. The nonmonetary value can be even more immense. With online voting the danger is actually much worse because anyone on Earth, including foreign governments, could derive great benefit from tampering with with U.S. elections, especially since it is unlikely the attackers will be brought to justice. Online voting fraud is thus a *national security risk* in a way that ecommerce fraud simply is not.

4. Conclusion

The sum of all of these considerations is simple. Although ecommerce transactions and online voting transactions are superficially similar, the security, privacy, authentication and transparency requirements for online voting are much more complex and stringent. The acceptability of small losses and the strategies for managing risk must be very different. And it is hard to grasp the full implications of the fact that online elections might be compromised and the wrong people elected via silent, remote, and automated vote manipulation that leaves no audit trail and no evidence for election officials or anyone else to even detect the problem, let alone fix it.

These points are all pretty basic, and they are not going to change for the better any time soon. While there is plenty of research going on in the computer security community to try to deal with the security and privacy problems of Internet voting, there is no technology on the horizon that is going to resolve them all in the foreseeable future. For the time being we simply cannot provide satisfactory security for online voting even though we can for online commerce.

5. Acknowledgement

Thanks to Prof. Candice Hoke for invaluable help in framing these issues.