Dr. David Jefferson
Computer Scientist, Lawrence Livermore National Laboratory[1]
Board Chairman, Verified Voting Foundation
Member, Board of Directors, California Voter Foundation
d_jefferson@yahoo.com 925-989-3701

The Dangers of Email and FAX Voting[2]

In the U.S. today there is widespread push toward Internet voting. Unfortunately, while it can be reasonably safe to transmit *blank* ballots over the Internet, the transmission of *voted* ballots over the Internet is a major national security risk, and really should not be considered for the foreseeable future with the kinds of technology we can see today. The specific risks of Internet voting are difficult to explain in short form because there are many architectures for online voting systems, and because the number of possible attacks is simply enormous. But if we confine our attention to *email voting,* the transmission of voted ballots as email attachments, then the dangers are easily explained.

In this paper we also include FAX voting in the discussion since, from a security and privacy point of view it is essentially the same as email voting. Although there are some differences, they share all the same kinds of vulnerabilities. And most jurisdictions that accept fax votes actually do so through an Internet fax service anyway, rather through an ordinary business fax machine connected to a telephone line, because fax machines are way too slow and can lose an incoming ballot because of a busy signal, paper misfeed, power failure, or because it runs out of paper or toner, etc.

Email and fax voting are by far the most dangerous forms of voting ever implemented in the U.S. Neither the Internet itself, nor voters' computers, nor the email or fax ballot collection servers are secure against any of a hundred different automated cyber attacks that might be launched by anyone in the world from a self aggrandizing loner to a foreign intelligence agency. An attack can be automated to modify or discard of any or all of the votes transmitted. Among all forms of Internet voting, email and fax are by far the easiest to compromise. To put it bluntly, an emailed ballot is about as vulnerable as a hundred dollar bill attached to a postcard sent through conventional mail.

The technical points I am about to make are not my opinions alone. The computer security research community in the U.S. is essentially unanimous in its condemnation of any currently offered forms of Internet voting, but most especially of email voting. In what follows I detail many problems with email voting and related technologies. I urge legislators regulators, and election officials to take the time to understand these concerns and to act accordingly.

---

[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, which takes no position on these issues.

1) Complete loss of vote privacy: A fundamental fact about public email and fax is that they are always transmitted in the clear, never encrypted.[3] This means that any IT person who maintains the email or fax server (with what is called "root" access to it) can read or copy anyone's email or fax freely. That includes both the ballots themselves and the voters' names. The same is true for anyone who maintains any email or fax forwarding agent along the path from the voter to the local election officials. Technicians at Google, Microsoft, Yahoo, AOL, and other large email providers have complete access to the ballots sent by their GMail, Hotmail, Yahoo Mail and AOL Mail subscribers. Likewise, technicians at Comcast, Earthlink, RoadRunner, Verizon, AT&T and other Internet service providers (ISPs) can do the same. And those are just the first-tier U.S. companies. There are numerous smaller U.S. companies and foreign corporations that handle email and fax traffic as well. We must recognize that it is simply not possible to guarantee the privacy or integrity of email or faxes.

Many voters (including many military voters) get their Internet service through their employers, who legally reserve the right to copy and inspect all incoming and outgoing email transmitted through their infrastructure. That would include emailed ballots along with the names of the voters who cast them. It is also routine for national intelligence agencies (including our own) to collect and store all email that crosses national boundaries, and sometimes a lot more email than that. The net effect of this is that emailed ballots are not only *not guaranteed to be private*, they are in many cases *guaranteed not to be private*. Most citizens have no idea how completely open email really is.

Some states that permit email or fax voting already recognize that privacy simply cannot be guaranteed for emailed ballots, and require voters to sign a waiver acknowledging that their loss of privacy. But that practice is of dubious legality, and is in any case inadvisable because the loss of voting privacy brings with it the concomitant dangers of automated vote buying and selling and of systematic vote coercion. These dangers are common in other countries and used to be common here as well until the mechanisms to provide strong ballot secrecy became nearly universal. However, if vote secrecy is widely compromised through email voting we can expect vote buying and coercion to return to this country, and be more widespread and automated this time around.

2) Vote manipulation while in transit: Because email and fax traffic is not encrypted, it can not only be read and copied while in transit from the voter to the local election officials, it can just as easily be modified or manipulated in transit en masse. *All of those companies that handle email traffic and are in a position to read or copy ballots are also in a position to modify them.* It is simple for any IT person who controls one of those routers or forwarding agents to filter out of the vast stream of packets exactly those that contain emailed ballots sent to the particular email addresses to which ballots must be addressed. He can then design a simple program to either discard ballots that contain votes he does not like, or spoil them with an overvote, or replace them with forged ballots that he likes better, all

---

[3] Encrypted email systems are widely available, but they require the secure generation, storage, and management of encryption keys, an IT task too complex and requiring too much knowledge and skill for all but the most technically adept voters to master by themselves. Only inside large defense enterprises with trained IT staffs is encrypted email routinely available to ordinary users. Generally speaking encrypted email would require each voter to either (a) pre-establish a secret symmetric encryption key shared *via some secure means* with his local election officials, and then install that secret key so it is available to the voter's email program or (b) download a certificate containing the local election officials' public key, install it so it is available to her email system, generate her own private/public key pair, install the private key so that it is available to the email program, and finally, register the own public key with a certificate authority known to and trusted by her local election officials. And the election officials would have to support this process on their side of the communication. The exact procedures will differ somewhat for every different email program that might be used by voters, of which there at least a dozen common ones and many more uncommon ones. For that reason no generic directions for how to do all this can be written, and voters will be on their own. Furthermore, many email programs do not support encryption at all, including almost all web-based mail systems and most tablet or smartphone systems. *People who do not understand the contents of this footnote will probably not be able to make use of encrypted mail.*

the while keeping the voter's signed affirmation and other attachments intact. This would only result in additional transmission delay of a few seconds, which would be completely unnoticeable.

Please do not think that on-the-fly email or fax manipulation is difficult. There are tens of thousands of people in the U.S. who have sufficient skill and are in a position to do this easily for at least some ballots, and vastly more people in other countries who could do it as well. Unless we completely give up vote privacy and publish all of the ballots along with the names of the people who cast them there would be no way at all to detect on-the-fly ballot manipulation. Neither voters nor election officials are in a position to notice any irregularity at all. It would essentially be a perfect crime.

3) PDF format: Although emailed ballots can in principle be sent in any of a large number of formats, for various reasons it is common to encourage or require the use of PDF (Portable Document Format by Adobe Systems, Inc.). Some people are under the impression that ballots in PDF form cannot be edited or modified, but this is completely false. While there are no general-purpose editing standards or tools for PDF, it can be arbitrarily modified like any other data file with custom tools.

PDF is an extremely complex data standard. As a result there is more than one way to represent a voted ballot using PDF. And because of that complexity most software tools support the PDF standard only incompletely. Different election jurisdictions and different voters are likely to use different tools to produce and process PDF ballots, and the resulting mix of not-so-perfectly interoperating PDF software can be disastrous. In the Oct. 2010 pilot Internet election in Washington, D.C. a voted ballot was represented as two PDF "layers", one layer for the blank ballot and another overlay layer for the marks that filled the ovals to represent actual votes. Unfortunately, most browsers' built-in PDF support does not fully implement PDF layering. The result was a horrendous design error that escaped initial testing. Had that system been used in a real election most voters would have unknowingly submitted completely blank ballots because the layer containing the vote marks was discarded by their PDF software.

PDF as a data format has other even more serious problems as well. It can carry malware, as we describe next.

4) Ballot files can carry malware into the election network: While many voters are somewhat familiar with PDF files, it is not widely known to the general public that PDF has one of the longest security rap sheets of any document type.[4] Innocent looking PDF files are able to carry very dangerous malware that can open a backdoor to remote control of the computer that processes them, in this case an election server. Once a vendor or local election official sets up a server to receive emailed PDF ballots, anyone can launch an attack by sending a specially-constructed PDF "ballot" carrying malware. That "ballot" email will be accepted into the election server like any real ballot, being admitted through all firewalls just as any other ballot. But once it is opened for processing, it will do whatever the attacker wants. This is a little like mailing in a paper ballot sprinkled with anthrax powder. There are ways to partially ameliorate this, but doing so greatly increases the development cost and operational complexity of the vote collection infrastructure, much as partially protecting the U.S. mail from anthrax increases costs and complexity in the paper world.

---

[4] See, for example,
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_rise_of_pdf_malware.pdf
or
http://www.blackhat.com/presentations/bh-europe-08/Filiol/Presentation/bh-eu-08-filiol.pdf

5) Server penetration attacks: Anyone in the world can mount a remote *penetration attack* on a server collecting emailed votes (or intermediate email servers, etc.). A penetration attack aims at taking remote control of the server, so that it obeys the attacker's remote commands and does whatever the attacker wants. The PDF malware attack described above is just one of many penetration attacks. If the attackers are competent and determined there is essentially no chance of election officials defending successfully. Current technology gives insurmountable advantages to attackers.

Almost all major high tech companies and government agencies in the U.S. have been victims of penetration attacks, including RSA, Google, Adobe, Lockheed-Martin, and the White House. These organizations all have security expertise, budgets, and infrastructure dwarfing that of any voting system vendor or election jurisdiction, and yet they have proved vulnerable to extremely damaging attacks that went unnoticed for months and whose perpetrators were never identified, let alone brought to justice.

In October, 2010 the Washington, D.C. Board of Elections and Ethics (BOEE) was forced to cancel its planned November Internet election because security researchers proved that they could easily penetrate the BOEE network while sitting remotely at the University of Michigan. They were able to take complete control of the servers, replacing all the voted ballots with phony ones, and were not detected until they revealed the attack themselves.[5] Although this was not an example of an *email* server being compromised, there is no essential difference. They could have attacked an email server located in the same data center just as easily.

6) Voters' computers infected with malware: Voters' own computers, as we all know, may be infected with malware. If email voting becomes common, nothing prevents an enterprising malware designer from creating, spreading and even selling a malware tool designed to sit silently on a voter's computer until the voter sends an email to one of the particular addresses that is used for emailed ballots. At that point the malware might modify the `To:` address just as the email leaves the computer in order to route the ballot to the malware-designer's own shop for inspection and modification before forwarding it on to election officials. Again, please do not think this is hard. It takes a little skill to spread malware, but it is much harder to detect than the attacks on the vote servers.

7) Denial of service attacks: Email can be subject to *denial of service (DOS) attacks*. It is easy, for example, to have a million emails sent to the voting email address, vastly swamping the relatively small number of legitimate ballots that a jurisdiction might expect. The overwhelming load can possibly crash the server by saturating some resource, or overload the human staff with the task of distinguishing real from phony ballots by hand. Anyone who owns or rents a large botnet (a collection of infected PC controlled by a criminal organization) can do this easily from the safety of overseas locations that are essentially untraceable. If a DOS attack lasts for the final hours of election day, the genuine emailed ballots arriving during those hours may be lost entirely or else delayed until it is too late to count them, and many voters can be disenfranchised. A denial of service attack happened in a Canadian election in 2003, crashing its servers for some time on

---

5 Wolchuck, Wustrow, Isabel and Halderman, "Attacking the Washington, D.C. Internet Voting System", *Proc. 16th Conference on Financial Cryptography & Data Security*, Feb. 2012

election day. The same thing happened again in Canada in 2012[6] and also in Hong Kong in 2012[7]. And in May 2007 a coordinated set of DOS attacks brought down many Estonian web sites simultaneously, including that of the Estonian parliament, along with Estonian banks, ministries, newspapers and broadcasters[8]. Had an online election of any kind been in progress at the time it would likely have been widely disrupted. Today it is easy to launch an even larger DOS attack.

8) Email and FAX ballots are unauditable. Attacks are undetectable and irreparable: Email and FAX ballots, like those cast on paperless DREs, are completely unauditable in any meaningful way. Without a voter-verified paper copy of each ballot snail-mailed back to local election officials there is no way, even in principle, to verify that a ballot arriving at the election server is the same as the one the voter intended to send. The attacks described above (except for denial of service) are likely to be completely undetectable. The wrong persons might be elected, the wrong initiatives passed or rejected, and no one would ever know! Even if an attack were somehow detected there is no way to know which votes were modified or discarded, so there is no way to repair the damage. And if someone publicized a false claim that email ballots were manipulated, there would be no way to prove that they were not. An unsubstantiated claim would probably not result in overturning the election, but such claims have a way of taking on a life of their own and undermining confidence in the legitimacy of the election and souring the public on the democratic process.

9) Multiple simultaneous attacks: We have to understand that an email election (and any other form of Internet election) might be attacked by multiple independent people or groups who may not even be aware of each other. This makes effective defense even more hopeless.

10) Similar problems with FAX voting: While FAX and email seem superficially different, they are in fact very similar from a security point of view even when the fax does not travel over the Internet. Faxes are transmitted unencrypted and they are forwarded from switch to switch within the telephony infrastructure of many private and national corporations, so it is impossible to guarantee FAX privacy. FAXes are subject to denial of service attacks from anyone with a computer. Generally, there is a FAX analog for each of the email vulnerabilities listed above, so fax voting is dangerous for all the same reasons.

11) Email and FAX voting are not just like mail-in absentee voting: Email and FAX voting may seem similar to mail-in paper absentee balloting with which we are all familiar and whose risks (although they are considerable) we are accustomed to accepting. But from a security point of view email voting is very different from mail-in paper voting. There is essentially no such thing as an *automated, programmed* attack on the integrity of mailed-in paper ballots, whereas that is a big danger for email and FAX ballots. There is also no such thing as a denial of service attack on paper mail. There is no such thing as "malware" that can modify a mail-in paper ballot before you put it in the envelope. Fraudulent reading or manipulation of mail-in ballots while in transit is not automatable, but has to be done one ballot at a time, requiring a either lot of work and time by one person to open, examine, modify, reseal, and resend many paper ballots, or else the cooperation and silence of many conspirators working together. And of course there are very strong laws protecting the privacy and integrity of all first class paper mail in most countries, but this is manifestly not true of email, for which there is often no legal expectation of privacy at all. The analogy between paper absentee balloting and email balloting just does not work when the security threats are considered carefully. It

---

6 https://www.theglobeandmail.com/news/politics/hackers-attack-ndp-delaying-in-electronic-leadership-vote/article2380413/

7 http://news.asiaone.com/News/AsiaOne%2BNews/Asia/Story/A1Story20120323-335323.html

8 https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

is enormously more difficult and risky to mount and hide an attack on paper mail than it is for email or FAX.

12) Other email issues: There are many other concerns with email addresses that do not fall into the category of security threats but nonetheless make email less attractive than might appear for ballots. Email addresses are trivially forgeable. People share email addresses regularly. People have multiple email addresses and change them frequently. Voters with multiple email addresses often forget to check all of them for mail, and may go weeks or longer between email checks on some addresses, or stop altogether. Email addresses can also be recycled, belonging first to one person and later to another. For these reasons email addresses should never be used as any kind of identifier for voters. If email voting were widely supported, there would be a temptation to collect email addresses as part of voter registration and use them for communicating with voters, but this would be a terrible headache. Keeping a current email address list is much more difficult than keeping a current postal address list because it is unlikely that voters will notify local election officials of a change in email address as they might for a change in physical address.

13) These facts will not change: These security problems are all facts of life about email and fax voting. They are fundamentally built into all standard email and fax technologies, into the architecture of the PCs and mobile devices that people might vote from, and into the Internet itself. These problems are not going to be "fixed" for as far ahead into the future as anyone can see, and we should not uncritically accept anyone's security claims to the contrary. No amount of encryption (even if described with the meaningless term "military grade"), no amount of firewalling, no use of strong passwords or two-factor authentication, and no other security tricks of the trade are sufficient to materially change these facts.

14) Recommendation: move toward Internet distribution of blank ballots for overseas and military voters: It is clear that overseas and military voters experience serious voting barriers that are largely associated with mail delays. While there are a number of cyber security issues regarding the electronic transmission of *blank* ballots to voters via the Internet, those issues are much more manageable than for *voted* ballots. I urge that states consider programs to reduce overseas mail delays by allowing voters to download blank ballots from a secure web server, then print them, *mark them by hand*, and snail-mail them back to local election officials. Such a process will eliminate at least one long distance or transoceanic mail delay. It will go a long way to relieving the problems of overseas voters without endangering the security of the entire election.