Hazards of Email Voting

David Jefferson
Lawrence Livermore National Laboratory
Board Member, Verified Voting
Board Member, California Voter Foundation
drjefferson@gmail.com
925-989-3701
April, 2017

From a security point of view email voting is about the most dangerous form of voting there is. It is easy for many parties to read or modify ballots *while in transit* from the voter to election officials. It is also easy to simply block selected ballots from being delivered. Such attacks can be *automated* to affect a large number of votes, and can be perpetrated remotely, by anyone on Earth, including criminal syndicates, domestic partisans, or foreign intelligence agencies. Neither the voter nor the election officials can detect such attacks, let alone prevent or correct for them. Basically, it is naïve and irresponsible to send any kind of secure or confidential document by ordinary email.

Russia has clearly demonstrated its capability to hack U.S. email, and the political willingness to do it. Other countries and our own domestic political actors have the same capability — it is not hard. *As you read the details of the potential threats below, imagine them being carried out by foreign agents or your political opposition*:

1) Email is not encrypted: Email such as voters would use from their home PCs or mobile devices is not end-to-end encrypted. Everything — the headers, the text, and the attachments (i.e. the ballot, voter identification, oath and signature) — are all sent entirely in the clear, and there is no good way around this. It makes email less secure than a postcard. This lack of encryption has many disastrous security consequences.

- **Ballots can be modified in flight to vote an attacker's choices:** Because it is unencrypted an email containing a voted ballot can be modified arbitrarily, or substituted, on the fly by malicious code anywhere along the path from the voters' computers to the county vote servers. Any IT person in charge of those email-forwarding servers (or other infrastructure) can do this, as well as any remote attacker from anywhere in the world who chooses to hack one that infrastructure. It is easy for an attacker to select, out of the millions of email messages passing through, exactly those that contain ballots, because they (and only they) are sent to the official email address(es) used for voting.

  This kind of attack has actually been demonstrated by Joe Kiniry of Galois, who showed that a remote attack on a home route could modify emailed

ballots in flight after they left a voter's computer. There is no protection against this at all, and no way to detect that it has happened.

- **Ballots can be selectively dropped in flight:** Lazy attackers don't have to go to the trouble to modify ballots in flight to affect the election outcome. They may simply throw away email *en route* that contain ballots with votes that they don't like. Again, neither the voter nor the receiver will know, at least until it is too late.
- **Ballots can be copied in flight:** Email containing ballots can be read or copied by anyone with control of a router or email forwarding server through which the ballot it passes. There are several serious consequences of this:

  (a) Vote privacy is completely lost, because the voter's name and email address are attached to the voted ballot.

  (b) Many people have their email service through their employer's infrastructure, and employers have the legal right to inspect and archive all email sent to or from employees through company infrastructure. This includes military personnel who would vote in the clear through military networks.

  (c) The loss of vote privacy enables possible large scale vote buying schemes, or coercion from employers, or may be used for future discrimination against voters who voted the "wrong" way.

  (d) Emailed ballots can be copied to third parties in flight. This would be valuable for domestic political operatives who want to know exactly who is voting for what or who want count the votes early to see how to invest their campaign resources during the last days of a campaign while balloting is in progress.

2) Email headers are totally forgeable and modifiable: The From: and Date: and other headers on email are not encrypted, and hence are totally forgeable or modifiable in flight. It is easy to send email that appears to come from someone else. (Spammers do it all the time.) And it is easy to modify the dates on email to make it appear that emailed ballots sent after the close of the election were sent earlier (and thus should be counted in states where the sending date is the criterion used).

3) Email offers no voter authentication: There is no way to verify the authenticity of an email, or that it actually comes from the voter it purports to. We have no national ID, nor any fingerprint or other technical means of authenticating email. Not only is the From: header completely forgeable, but even if the voter is required to provide some additional private information (such as birthdate, SSN, driver's license number, or password of some kind) that is a very weak kind of authentication. Hundreds of millions of people's private information has been compromised already via many commercial cyber attacks that have made news in recent years. And if private information is sent along with the ballot, it is sent in the

clear (unencrypted) like the rest of the email, so an attacker can collect that private information while also substituting a ballot containing votes that the attacker likes.

4) Email does not offer a way to send wet ink signatures. Voters must accompany their email by a signature that can be compared to the one on file in the voter registration database. However, of course, in email it can only be a facsimile signature, not an original wet ink signature. Facsimile signatures can be cut and paste from any other document, so attackers can easily forge large numbers of ballots if they have a trove of signature images from some earlier data breach.

5) Email is only a best efforts delivery service: Email is normally delivered in minutes, but this is not guaranteed. It is a "best efforts" delivery service. Because ISPs do not charge for email, they feel no obligation to offer any speed guarantees. Email with attachments, such as a ballot, is often delivered much more slowly than email that contains only text. We are all familiar with cases where email has been delayed by hours or even days, a hazard that could effectively disenfranchise voters who sent the ballot by email in the last hours of Election Day. Email can also be removed or diverted by spam filters, but spam filters are imperfect, and might divert legitimate ballots, leading to additional delays or lost ballots.

6) PDF can be used to deliver malware to the server: Most email voting systems require the ballot and the user's identification to be in the form of PDF attachments to the email message. However, PDF is a notoriously dangerous file type because specially constructed PDF files can be used to deliver malware to whoever receives and opens it. An attacker could create a malicious PDF file that looks like a benign ballot but contains malware. When it reaches the election server it could introduce a backdoor for the attackers to gain control of the election server.

7) Email is subject to all the other generic attacks the Internet is vulnerable to: The above problems are just those specific to email voting. But there are generic attacks on Internet traffic of *all* kinds that affect email as well as all other kinds of communication. These include:

- *Denial of service attacks,* which can so clog a server with traffic that nothing can get through for several hours until defensive efforts can be ramped up. But several hours on Election Day can be the difference between thousands of ballots arriving on time vs. arriving too late to be legally counted. These attacks are notoriously easy to perform in a large variety of distinct ways, and there are whole dark businesses on the Internet that will conduct such an attack for you (for a price) if you don't want to do it yourself.
- *Server penetration attacks*, in which the attacker directly attacks the server that collects the emailed ballots and modifies, copies, or deletes ballots as the attacker desires.
- *DNS poisoning attacks*, which can cause ballots to be transmitted to the wrong place, so they never reach the election server at all.
- And there are many others.