Hazards of Email Voting

David Jefferson
Lawrence Livermore National Laboratory
drjefferson@gmail.com
925-989-3701
March, 2015

From a security point of view email voting is about the worst form of voting ever proposed. 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. Sending ballots by email is as dumb as taping a $100 bill to a postcard and expecting it to be delivered safely. Basically, it is naïve and irresponsible to send any kind of secure or confidential document by ordinary email.

In more detail, here are the technical facts.

1) Email uses no encryption: Ordinary civilian email such as voters would use from their home PCs or mobile devices is not end-to-end encrypted. The headers, the text, and the attachments (i.e. the ballot) 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 in the voter's own infected computer or mobile device, or in the voter's home router, or by malicious logic in any router or mail forwarding server along the path from the voter to the mailbox of election officials. Any IT person in charge of those routers or servers can do this, as well as any remote attacker from anywhere in the world who chooses to hack one or more of systems. This has actually been demonstrated (not that it was necessary) by Joe Kiniry of Galois. There is no fundamental protection against this at all, and no way to detect that it has happened. Furthermore it is easy for an attacker to select, out of the millions of email messages being transmitted, exactly those that contain ballots, because they (and only they) are sent to the official email address(es) used for collecting ballots.
- **Ballots can be selectively dropped in flight:** Lazy attackers don't have to go to the trouble to actually modify ballots in flight to affect the election outcome. They may simply throw away email messages that contain ballots with votes that they don't like, and let through emailed ballots they do like.

Again, neither the voter nor the intended receiver will know, at least until it is too late.

- **Ballots can be read or copied in flight:** Even if not modified or dropped 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) The loss of vote privacy enables large scale vote buying and selling schemes, or coercion.

  (c) 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.

  (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 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 is only a best efforts delivery service: Email is normally delivered in minutes, but this is not guaranteed. Email 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 (e.g. 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.

5) 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.

6) 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, e.g. the web. 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.