Andrea Gyger

From: Margit Johansson [redacted]
Sent: Friday, January 15, 2016 4:18 PM
To: SoS Rulemaking
Subject: Comment on Rules 1-15-16, 2:38 AM

Dear Secretary Williams and Staff:

This is a comment on existing Rule 16.2.8, that was written last year and states "Nothing in this Rule 16.2 permits internet voting. Internet voting means a system that includes remote access, a vote that is cast directly into a central vote server that tallies the votes and does not require the supervision of election officials."

This definition of the term internet voting is too limited. That is because it does not mention that returning one's voted ballot by email is also internet voting. Use of electronic mail, or email, is use of the internet. By eliminating email as part of the definition of internet voting, the Secretary does little to reinforce the intention of our legislation that more insecure methods of voting be used as little as possible, so as not to risk the accuracy of elections. Our 1-8.3-113(a) says electronic transmission (which includes email as well as casting one's vote onto a server) is only allowed "In circumstances when another more secure method, such as returning the ballot by mail, is not available or feasible, as specified in rules promulgated by the secretary of state;" Relative security of voted ballots affects whether voted ballots will be counted. The secretary of state is required to maintain the "purity of elections". We need an election official who, since not a computer scientist himself, cares enough about election integrity to be careful about whom he trusts for scientific information.

The voting public needs to be informed on how to vote most securely. Rules to date do not appear to have given the guidance to voters that is needed for them to vote responsibly.

Below is a page which computer security expert Barbara Simons (co-author of the book BROKEN BALLOTS) wrote to Colorado legislators when they were considering HB15-1130 on military and overseas citizens voting in local elections and using electronic return of voted ballots. It is well-worth reading.

Thank you for your attention to this matter.

Sincerely,

Margit Johansson
[redacted]

Risks of Internet Voting

Barbara Simons

simons@acm.org

[redacted]

All commercially available systems that allow voters to send their voted ballots over the internet, whether via email or a website, are insecure. Furthermore, there are no standards, and there is zero oversight or testing of internet voting systems by any state or federal agency. Typically, the software that runs the systems is secret, so independent computer security experts are unable to analyze the software for bugs, vulnerability risks, privacy violations, and election rigging malware. By allowing voters to use an insecure and unreliable system, we are making them second class citizens and putting our democracy at risk.

Some people think that attaching a copy of one's voted ballot to an email is less problematic than voting at a website, but that is not the case. Because the voter's name is on the email header, the voter is deprived of a secret ballot, opening up voters to the threat of coercion. There is also the increased risk of vote buying/selling.

Email is essentially never encrypted, so ballots sent as email attachments can be read and modified by anyone en route and at the receiving end. In addition, because it is easy to create large number of emails with fake "From:" headers, someone with access to a list of voters could submit thousands of forged ballots.

Another risk is that the voter's computer could be infected with election rigging malware that modifies the vote just before it is sent over the internet. (This is also a risk of web based voting). The voter might think that what she sees on her screen is what goes out over the internet, but that is not necessarily the case. Computers consist of many different components; the screen is only one. There is software between the screen and the link to the internet, and that software could modify a voter's selections without detection.

The threat of criminal malware on a victim's machine is not a theoretical risk. Millions, or even billions, of dollars have been stolen from online bank accounts by malware. The reason we don't hear much about this is that banks quietly cover the losses, because it is cheaper than building new buildings and hiring new tellers. For example, the Zeus Virus, which has stolen vast sums of money from online bank accounts, is so smart that when the victim looks at her online bank statement, it seems correct, even though the money may be in Timbuktu.

Since customized versions of Zeus are available on the black market, and since simply modifying a vote is far easier than stealing large sums of money undetected, the possibility of a Zeus-like virus infecting voters' machines is a real threat.

There are many other risks associated with email voting, including denial of service attacks that overwhelm the election official's machine. In addition, since voted ballots are likely to be sent as pdf attachments, there is the risk that someone wanting to attack the election might infect the election official's machine by sending a fake ballot containing malware in the pdf attachment. (Pdf is known to have security vulnerabilities).

A good thing to keep in mind whenever anyone claims that software is completely secure and reliable is that large software vendors, such as Microsoft and Apple, send out frequent software updates, many of which are to repair security holes in the software. If large wealthy companies with vast numbers of smart programmers are unable to write completely secure and reliable software, why should anyone believe that far smaller voting system vendors can achieve what Microsoft cannot?

In conclusion, because of the risks of software bugs and malware, whenever computers are used in elections, we need to have a way of checking them–ideally a risk-limiting manual post-election ballot audit. But, it is impossible to check the correctness of internet elections, because it is impossible with currently available commercial systems for the voter to verify that the version of an internet ballot received by an election official is identical to the ballot the voter thought she was sending.