# What happened in the Utah GOP Caucus

Matt Bernhard


*Note: this originally appeared as a Medium post here*

Thousands of people went to the polls on Tuesday to vote in the 2016 presidential primary and caucus races. In the state of Utah, the Republican Party used an Internet voting system to augment their in-person caucus, with the hopes that it would make voting significantly easier for members of their party. Unfortunately, the complexities of the Internet do not create a sufficiently secure environment with which to entrust our Democracy, a fact that has been noted time and time again by numerous experts in the fields of computer security, cryptography, and voting systems (for a detailed breakdown

of what factors into Internet voting and voting technology in general, see this). The Utah GOP caucus was no exception to this rule.

The system had numerous vulnerabilities despite being a good-faith effort in producing a usable, accessible, secure, and accurate online voting system. The vulnerabilities stem from the architecture of the system, from the specific Internet technologies it relies on, and from other problems external to the system including social engineering and coercion issues. To better examine these issues and attempt to communicate the underlying reasons for them, we will walk through the system step-by-step as a voter would during the election process.

## Registration

Voter registration for the caucus (both online and in-person) closed on March 15th, one week before the caucus. Registration was facilitated via EventBrite, a third-party commercial event-planning website. Voters could visit EventBrite's site, search for their county and terms relating to Utah, GOP, Republican, and caucus, and they would be led to a page which had a form requesting the voter's name, email, birthdate, address, phone number, and how they would like to vote (online or in person). After registration, voters receive a PIN to the provided email and/or phone number. Once the voter fills in their information, they get a confirmation from EventBrite via email:

There are a few problems here. One, this email is in no way official confirmation of registration (an enormous usability issue). I attempted to register myself after the March 15th deadline, with absolutely no shot at eligibility in the election (I'm registered to vote in Texas), and received the above email. A few days later, I received another email from the Utah GOP itself informing me that I was not eligible to vote, as I was not on their voter rolls. Had I thought I *was* eligible to vote, and if I had never received the second email, you can see how this could be confusing.

Since the event registration is not authenticated, anyone can register anyone else to vote through EventBrite, provided they have the necessary details about the person they are trying to register (note: this explicitly violates the GOP's caucus rules laid out here). What's more, all of the information you need to register any eligible voter is available in the voter database that can be purchased from the state for $1050. This means that any motivated individual with modest financial resources (say, a candidate who's been trailing in the forecast polls) could register any likely voter. According to the EventBrite site, if you register to vote only online, you will be ineligible to vote in person in the caucus (though it appears this rule was not enforced). Effectively, by using the voter database, you can disenfranchise every voter in the Republican caucus by either making them ineligible to vote in person or by stealing their voting PIN and preventing them from voting online. Voters or groups of voters can also be targeted; if you know a voter or group of voters who are voting for a certain candidate, you can make sure they are not able to do so. While it is doubtful that an election scale attack occurred preventing people from voting, there have been numerous accounts of people not getting their PINs, and thereby not getting to vote online (See here, here, and here for a few).

## Voting

After registration, voters are asked to go to the website ivotingcenter.us in order to submit a ballot online. Notably, several domains with names very close to this were still available to purchase as of a few days ago, and we snapped up ivotingcenter.gop and votingcenter.us (which are still up if you want to take a look, and were picked up in a few blogs). While our sites simply redirect voters to the correct voting website, it is perfectly conceivable that a malicious party could use one of these sites to trick voters into not actually voting, steal their information, or create other malicious outcomes through a domain squatting attack.

As for the actual security mechanisms of the voting site itself, the site does seem to be relatively secure. It receives an A- on SSLLab's tests for the strength of its encryption configuration (notably, our site received an A). The main reason it does not receive full marks is that it does not provide perfect forward secrecy in all browsers, which means that if an attacker at any point in the future breaks the encryption for any voter's voting session in a vulnerable browser, she can then see how that voter voted. The voting application appears to use elliptic curve and ElGamal homomorphic encryption, and the use of a blockchain, which secures votes as they are transmitted and through the vote tallying process. Additionally, the architecture of this encryption system enables voters to verify that their votes recorded properly. By visiting a verification site with a special code corresponding to their vote, voters can make sure that the system properly recorded who they voted for by making it reveal their vote.

## Verification

In general, being able to prove who you voted for in any secret ballot election is a bad idea, as now anyone who knows you can coerce you to vote a specific way. There are two main outcomes from this: either votes can be bought, with a motivated party asking voters to prove how they voted for financial compensation, or motivated parties can intimidate people to vote a certain way, *or else*. "Or else" could mean any consequence severe enough to make a voter change his behavior, but the major takeaway from both cases is that every citizen does not to get to express their opinion to the full extent of their rights.

Notably, regarding our domain squatting attack, we could squat the verification bulletin board, and thereby know how any voter voted if they mistakenly gave us their voting receipt number. This defeats the secret ballot, which is widely considered one of the most significant advancements in democracy in human history.

## Other failures

The system, as many large online public infrastructure type systems have before (think healthcare.gov), did not get off to a running start. The site was programmed to go live at 7 AM Mountain Standard Time on the morning of the election, i.e. when the polls officially open. Unfortunately, Daylight Saving Time went into effect two weeks prior to the election, so the system was down for the first hour of voting. After the site came up, there were also several outages, and even the YouTube videos meant to help explain the process went down.

The GOP tried to offer support through a phone line and online chat service in addition to the educational resources on their website. The chat service obviously did not work when the site was down, and the phone service appeared to have outages as well (see here and here).

## Conclusions

In short, experts have warned against Internet voting numerous times in the past, and yet again have been proven right. There were even warnings about this particular election beforehand. Voting systems are enormously complex, and the intricacies of the voting process are only compounded when adding in another enormously complex system, the Internet. As has occurred in Washington, D.C., Estonia and New South Wales before, experience has shown yet again that we do not yet have the sophisticated technological infrastructure to support an online election adequately. The security challenges are very steep, and even simple resource and infrastructure management proves to be a very difficult problem when attempting to serve tens of thousands of ballots in a secure manner. There will come a day in the future when Internet voting becomes a reality without any of the major flaws and vulnerabilities we have seen so far. However, that day is still a long way off.