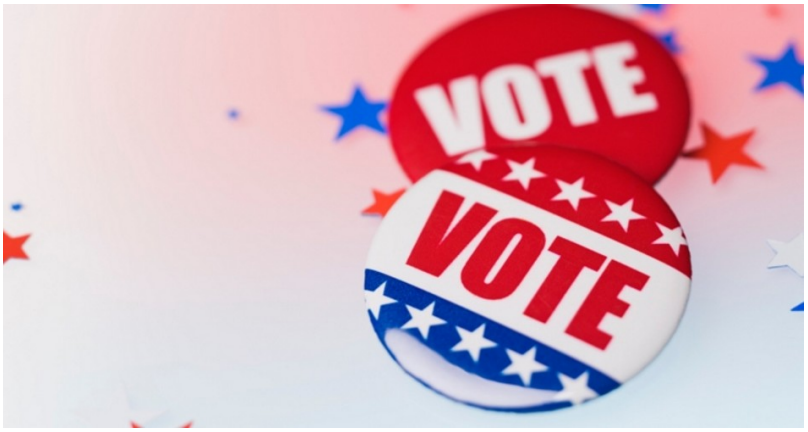
Written by **Kurt Hyde** on March 22, 2016

Utah GOP Uses Internet Voting in Presidential Caucus



Utah Republicans are scheduled to begin their caucuses this evening at 7:00 p.m. MDT, but the balloting will already be underway via Internet voting when the caucuses begin. Even after the in-person caucuses end, the Internet voting will continue. The Utah GOP website says the online voting will be open from 7:00 a.m. until 11:00 pm.

Many computer experts have spoken out against online voting owing to the security vulnerabilities inherent in the Internet. A chain is only as strong as its weakest link, and no matter how many security features are incorporated into the election hardware and software, inserting the Internet into the voting system puts a weak link into the voting process.

Readers of *The New American* were warned of a number of Internet vulnerabilities in the October 9, 2000 issue in an article entitled "Voting on the Web." The Arizona Democratic Party had experimented with Internet voting in their primary in March of that year. Joe Mohen, who was the CEO of election.com at the time, was interviewed by *The New American*. He broke the news that there had been e-attacks attempted in that primary. The two types of e-attacks that were detected were successfully thwarted: password guessing and denial-of-service. Of course, the unanswered question is, how many other e-attacks were there in that election that were not detected? Hopefully they were all unsuccessful.

On January 21, 2004, computer experts Dr. David Jefferson, Dr. Aviel Ruben, Dr. Barbara Simons, and Dr. David Wagner published a report entitled "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)." SERVE was an Internet-based voting system intended for voting by the U.S. armed forces. In their report they stated, "Because SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc.), any one of which could be catastrophic."

We must consider the obvious fact that a U.S. general election offers one of the most tempting targets for a cyber-attack in the history of the Internet, whether the attacker's motive is overtly political or simply self-aggrandizement.

A presidential primary or caucus would be just as tempting a target as a general election. The stakes are high and the costs are high. That means even a relatively high-cost e-attack is likely to be economically feasible under such circumstances.

The New American reported on October 27, 2010, on the now-famous successful white-hat hacker e-

attack on the pilot project for Washington, D.C., online voting. "White-hat hacker" is a term for a person who hacks into computer systems, usually with prior permission, for the purpose of finding vulnerabilities and reporting them to people who can fix them.

The white-hat hackers from the University of Michigan hijacked the voting system and were in control of it undetected by the elections officials who were conducting the test. The white-hat hackers published their findings in a paper presented at the 16th Conference on Financial Cryptography and Data Security in February of 2012:

> In 2010, Washington, D.C. developed an Internet voting pilot project that was intended to allow overseas absentee voters to cast their ballots using a website. Prior to deploying the system in the general election, the District held a unique public trial: a mock election during which anyone was invited to test the system or attempt to compromise its security. This paper describes our experience participating in this trial. Within 48 hours of the system going live, we had gained near complete control of the election server. We successfully changed every vote and revealed almost every secret ballot. Election officials did not detect our intrusion for nearly two business days — and might have remained unaware for far longer had we not deliberately left a prominent clue.

The "prominent clue" was to have the website play the University of Michigan's fight song "The Victors" after each ballot was cast. Needless to say, hackers planning to alter the outcome of an election would not have made their attack known. They would have accomplished their goals and then erased their tracks.

Beitbart News reported Monday that it had concerns regarding the management at Smartmatic, the company that is supplying the software for the Internet voting portion of Utah's Republican Caucus.

The chairman of Smartmatic's board, Lord Mark Malloch-Brown, currently serves on the board of George Soros's Open Society Foundation and has close ties to the billionaire.

Another concern is who is authorized to access to the database of ballots that have been cast. *The New American* has contacted the Utah Republican Party headquarters in Salt Lake City asking if they intend to make public the names of all individuals who have privileged access to that database of ballots. Even those who have read-only access to the ballots have the ability to scan the cast ballots and obtain inside information on how the election is going. As of press time for this article, the Utah Republican Party has not yet responded to that request.

Another concern is vote buying. If people can vote on their PCs, laptops, or other portable devices, that would be an opportunity for buying and selling votes since vote buyers would be able to watch vote sellers as they cast their ballots without meaningful opportunity for election observers to catch this.

The *Wall Street Journal* on Saturday said, "Voters will get a receipt that will verify that their vote was recorded correctly." *The New American*, in the same inquiry as above, also asked if this receipt would be given to voters to take with them. If the receipt is given to the voter instead of being retained under proper controls for a recount, that would also assist in vote buying. As of press time for this article, the Utah Republican Party has not yet responded to that request.

Vote buying is still possible with precinct voting, even with paper ballots, but it is made substantially more difficult by having the voting in a limited number of publicly known locations where election observers inside or directly outside can look for the tell-tale signs of vote buying. Precincts were established for voting because they are a fundamental building block of honest and accurate elections. Precincts should be preserved.

The State of Utah studied online voting and produced a report dated August 21, 2015. This report, while not as strongly worded as some computer professionals would like, still had this in its conclusion: "The problem is that Internet voting also possesses numerous inherent security risks that must be mitigated before it is implemented."

Among those listed in Utah's iVote Advisory Committee is Lieutenant Governor Spencer Cox, a Republican, as well numerous other Republicans and Democrats in Utah. Why is the Utah Republican Party doing something in their caucus that the State of Utah has cautioned against doing in their elections?