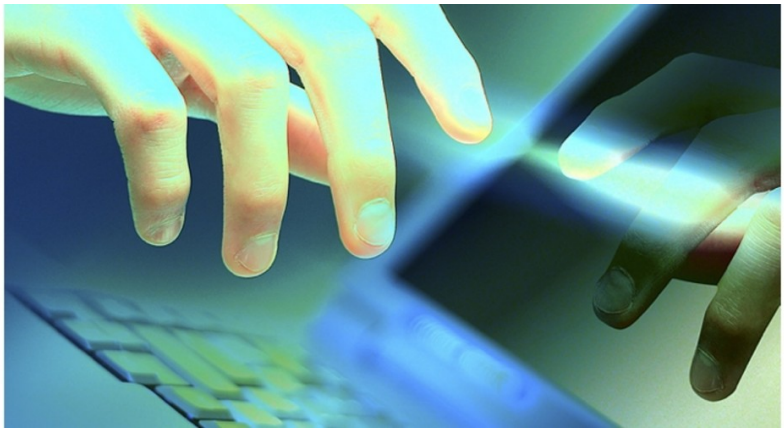
Written by **Kurt Hyde** on November 4, 2014

Dangers of Internet Voting



Yesterday's *USA Today* had an article entitled "Internet Voting 'not ready for prime time.'" The story quotes Verified Voting as saying that there are about three million people eligible to vote online in today's elections, most of them members of the military. Numerous security risks are cited that are inherent in Internet voting.

Readers of *The New American* have often been warned about the dangers of Internet voting. For instance, the October 9, 2000 issue carried an article entitled "Voting on the Web," in which readers were told of the dangers to electoral integrity due to the inherent insecurity of the Internet.

Back in 2010, Washington, D.C., experimented with a new online voting system. City officials were so confident their set-up was secure that they invited the public to attempt to hack it. University of Michigan graduate students Eric Wustrow, Scott Wolchok, and Dawn Isabel accepted the challenge and, working with Professor J. Alex Halderman, were easily able to break into the system. Their published report revealed:

> 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 clue they left was an audio recording of the University of Michigan's fight song, which was played on the thank-you page for the voters after casting their ballots. The hackers were also able to capture passwords.

Fortunately, these were not malicious hackers. So-called white-hat hackers penetrate a system for the purpose of identifying security weaknesses, and then publish reports and propose improvements.

Many people have asked why they cannot vote via the Internet, when they can pay their bills using their laptops or smart phones. The reasons are legion, but one should stand out clearly. Paying a bill is not a secret ballot transaction. There are ID numbers attached to payments for traceability. If a bill payment fails, a consumer can be contacted by the business to resubmit a payment.

There are a great number of security weaknesses in Internet voting: no voter-verified paper audit trail, denial of service attacks, spoofing, eavesdropping by servers along the way capturing people's passwords and enabling verification of vote selling, just to name a few. There are also security weaknesses in the user devices such as laptops or smart phones. They include key-stroke monitors, stored passwords, and many others. There are numerous special interests in both the United States and foreign counties for whom the outcome of our elections is of major importance. They have the

resources to exploit these security weaknesses, and it's well worth their investment.

But the greatest danger of stealing elections is from inside, not outside, attacks. In almost every case of vote fraud that is investigated, there's at least one insider, a supposedly trustworthy individual, who plays a key role. Internet voting, in addition to its vulnerability to outsider attacks, is wide open to fraud committed by people with privileged access to the computer system. It might be the system administrator, the application administrator, the programmers, or those in charge of generating the passwords for the voters. If these people are appointed either by elected officials or by people who owe their jobs to elected officials, there can be a conflict of interest involving election results.

Look at how easily some congressional legislation could be used for fraudulently manipulating an election.

National Defense Authorization Acts have been used many times for politicians' pet projects. The NDAA for 2012 caught the public eye when opposition rose against the provision for indefinite detainment of American citizens. A lesser known dirty trick rider was placed in the NDAA for 2010. Section 589 of HR 2647 was entitled Technology Pilot Program. Under the innocent-looking phrase one can find the following:

> The Presidential designee may establish 1 or more pilot programs under which the feasibility of new election technology is tested for the benefit of absent uniformed services voters and overseas voters claiming rights under the Uniformed and Overseas Citizens Absentee Voting Act.

It gets worse:

> In conducting a pilot program established under subsection (b), the Presidential designee may consider the following issues:
>
> > The transmission of electronic voting material across military networks; and virtual privet networks cryptographic voting sytems, centrally controlled voting stations, and other information security techniques.
> >
> > The transmission of ballot representations and scanned pictures in a secure manner.

This is the federal government specifying Internet voting. Note that the person in charge is a "Presidential designee." Nowhere in the U.S. Constitution is the president authorized to appoint someone to run an election. Aside from the security problems inherent in Internet voting, it is unconstitutional for the federal government to order Internet voting for anyone. Voting is meant to be run by the states.

The U.S. Constitution does not grant power to the federal government to authorize overseas voters. While the number of such voters is currently small, it could grow in the future. Overseas voters are virtually impossible to verify by election integrity advocates.

Bottom line: The current state of Internet voting is verifiably unsafe and it shouldn't be used in elections. The portion of the NDAA for 2010 that specifies Internet voting should be repealed.