Online Voting is Technically Ready

Our Experience with Elections, Technology, and Security

Konnech' Inc.

NASS White Paper

February 2015

Contact: Laura Potter

(800) 381-1499 Ext. 205

Laura@konnech.com

your election konnection

| (517) 381-1830 | (877) 301-0793 Fax|
4211 Okemos Road Suite 3 & 4| Okemos, MI 48864|
www.konnech.com

Introduction

Based on our experience working with state and county electoral administrators, as well as our familiarity interacting with different vendors, we strongly believe that online voting is technically ready. In a world of near-infinite computing power, ubiquitous connectivity, cloud-based services, and big data, why are the same technologies that have revolutionized so many aspects of our daily lives not being used to improve the electoral process?

Analysis

Viewed principally as a transaction, voting has some unique aspects. Financial transactions depend on creating a secure, reliable, and auditable end-to-end process that infallibly links, for example, buyer to seller. That entails creating strong, secure, and transparent identities for each party to the transaction. Online voting, by contrast, is predicated on privacy, anonymity, and freedom from outside influence or coercion—but also on the absolute auditability that is necessary to guarantee the principle of "one person, one vote" and to verify that each voter's intent is reflected in the election's outcome.

Since there is no way to authenticate a voter's actual identity until that voter is onsite, online voting challenges continue to remain. Authenticating (credentialing) presents significant challenges in the current environment and these challenges are exacerbated by the sheer number of devices and possible limitations in voter interfaces. Implicit or explicit mapping between online voting device identities and voter identities will be required; yet this must be done without compromising the secrecy of the vote.

Today more and more voters are using a multitude of online election services: submitting voter registration applications (to include FPCA), updates to registration records, absentee requests, poll worker applications and poll worker training. For each access to these online voting services, it is currently possible for the jurisdiction web server to know the online user's virtual identity factors-- IP address, network router(s) and hardware ID(s)-- and have them linked to the voters' application information. Election after election, the jurisdiction server can accumulate a large number of these Virtually Profiled Voters (VPV). For these VPV, the server or the Voter Identity Management System (VIMS) can give each person a score based on a certain mathematic model. This solution will solve a critical issue for online voting - ensuring the voter identity. In addition, if the VIMS is allowed by the voter to track the voter's key striking speed and mouse movement pattern, the individual behavioral data will make the identification of a unique online voter easier and more reliable. Therefore the VIMS will give a voter a higher score.

If VIMS uses outside big data such as cellular user location data to identify one particular voter, it will enhance the score further. Using this score, the VIMS is in a good position to grant some VPVs immediate approval of online requests such as address change, absentee request, online ballot delivery, and ultimately online voting with paper ballot as the backup or even without paper ballot.

For a non-VPV online request or any virtual profile change, just as when you open a new online bank account or use a new computer to access your online bank account, a multiple channel verification such as a phone call or texting a message with a unique code is needed to start or to maintain a score. Once everyone agrees that the VPVs with a certain higher score should be considered authenticated, this group of voters will be granted online voting rights. As the VIMS matures and a large portion of voters reach the high VIMS score, the jurisdictions will be able to conduct online voting for this portion of the voters. The VIMS maturation for online voters is an iterative process.

It has become clear that election departments have already adapted to conducting most election related services online. Over the past few years, even the recruitment, training, and retention of poll workers has rapidly evolved to be done online. In one county over 80 percent of their poll workers enrolled online for training classes in the first month the service became available.

Since the online profiles accumulate over multiple elections, it will become almost impossible for one person to successfully impersonate another.

Again, if the system is in place to monitor all voters' online election activity starting from the date of voter registration, the system will be able to provide online voting service within the limitation of risk tolerance.

Challenges

For many jurisdictions, the creation of VPV presents a significant challenge. Currently, most electoral administrators are comfortable providing a few election services online, albeit one service and one vendor at a time. Voter registration, for instance, is usually conducted by one vendor, while the services of the UOCAVA ballot delivery, absentee requests, candidate filing, ballot preparation, ballot-by-mail, and election department web sites are provided by other vendors. In many cases, local jurisdictions use services provided by outside entities. Therefore, this vital election data is not accessible by one jurisdiction, or collected in one database.

A second challenge is that most vendors do not use a national standard. It is costly to combine information from multiply formatted web programs into one database. VIP and IEEE1622 groups have done a great job encouraging uniform formats. The move toward Election Markup Language under these initiatives is a critical component for allowing multiple data sets to be collected, collated, and analyzed.

A third issue that electoral administrators are uncomfortable with is tracking their voters' virtual identities through their online services. This is a completely understandable concern, as voter privacy and security are essential to ensure election confidence; however, this potential risk should not cause the election leadership to shy away from online voting. The election industry has the creativity, resources, and technology to create a safe, secure, and confidential online voting environment. The members of NASS will need to educate fellow administrators and the general public of that in order to make online voting a reality.

Solutions

Having worked with nearly every aspect of election technology, we firmly believe that online voting technologies are ready.

The voters are ready for more online activities too. The State of Montana's UOCAVA voters requesting electronic ballot delivery has increased 3.6 times in just 4 years. State and County election administrators are more and more confident about granting UOCAVA voters access to their ballots online, and administrators are able to approve most of their online voters in a real-time fashion. The feedback from Montana's UOCAVA voters shows that they not only are satisfied with their online voting experience, but that they are excited and eager about the possibility of online voting for future elections.

A simple tool performing a risk score calculation successfully alerts the DC Board of Elections (DCBOE) to potential problems. In our 2014 NASS conference White Paper co-authored by both the DC Board of Elections and Konnech, we discussed using some very simple data sets such as voter's IP address, network router ID, and email address to trigger alerts so the election administrators can quickly identify and focus on any duplicated or questionable applications. With a longer period of data collection, the alert tool will become much more sophisticated.

For future study, the voter behavior data (key striking speed, mouse movement pattern, etc.) creates a powerful tool to single out suspicious online events. The benefit of using this type of data is that more voters can be granted instant approval of their new requests. These experiences can be fine-tuned and ultimately give election administrators and voters the confidence that is required to safely and securely vote online.

We as an industry have to pay close attention to the data security of virtual voter identities and voter usage behaviors. This is critical because it is what will provide our voters with privacy and it will satisfy our electoral administrators that we can safely and securely conduct our elections online.

Conclusion

The online services provided by election departments across the United States has given vendors valuable experience and has built the technical infrastructure needed to evolve our voting process to the next step. Now it is the time to take another serious look at online voting.