

UOCAVA Solutions Working Group
Group A (Blue) Notes
Saturday, August 6, 2011

General Group - Attributes Discussion

- Arthur Keller - Questions on scope were asked. Concerns were expressed that this demonstration project may become a rollout of eventual Internet voting beyond UOCAVA voters.
- Tammy Patrick – A statement was made regarding the need to focus on the use CAC cards. The group disagreed and said we do not need to focus only on CAC cards as their sole use has not been pre-determined.
- Peter Zelechowski – It was said that we need to limit the scope of group discussion to military voters but CAC cards are not a requirement at present.

Breakout into three (3) tables:

Small Group

(Catherine Meadows, Elan Kaplan, Nelson Hastings, Lowell Finley, David Cary, Island Pinnick)

- See paper flowchart (Facilitators turned this into a PowerPoint slide)

Election Officials Strike Back

(Jeremy Epstein, Thad Hall, Sean Dean, Cyrus Walker, James Ott, Veronica Degraffenreid, Tammy Patrick)

- This group added things to the Small Group's overview which are now on the sheet / PowerPoint slide.
- The demonstration project must include voter registration, so we need to include sub-steps such as FPCA.

Team America

(Peter Zelechowski, Stacey Van Zuiden, Dan Wallach, Joshua Franklin, Aaron Lorenzen, Arthur Keller, Neal McBurnett, Alan Sherman)

- System Certification & Testing according to national and state standards and local acceptance
- Logic & Accuracy (L&A) Testing
- Ballot Definition
- Build the Electoral Roll – authenticating the voter, signature, ID, etc.
- Ballot Distribution – via mail, electronically, in polling place, etc.
- Ballot Marking – voter indicates intent
- Ballot Cast/Returned
- Ballot Interpretation/Merging and Tabulation
- Periodic Reporting
- Canvassing
- Auditing

- Certification

Lowell Finley (Small Group) – One view presented was taking the initial list that was passed out and only adding “Auditing” between “Return of Voted Ballot” and “Certifying/Canvassing”. It was stated that the lack of “Auditing” on the list was a significant oversight.

The Small Group and Election Officials Strike Back are in agreement with the chart on the piece of paper/PowerPoint slide. Team America likes their list captured above.

Jeremy Epstein – It was asked whether military UOCAVA voters with disabilities or those who did not speak English should be considered in this demonstration project. The group said yes, however is it not a requirement that all members of the U.S. Military read, write and speak English?

Cyrus Walker – Some in the group believe auditing to be procedural, not part of a voting system. There was much debate about that by the group. It was determined that the group did not want to get caught up in debating this point further and wanted to move ahead.

Perspective: Voter

Alan Sherman - Scope questions were asked again. It was determined that for the purposes of this exercise, we are ‘ignoring’ the civilian UOCAVA voters – even military spouses and family members - and focusing only on active duty military.

The group determined that we need to make sure there is no denial of service either electronically or by the post office.

Alan Sherman – There was a statement of concern that we are treating UOCAVA voters more specially than we are treating regular absentee voters. There was discussion around this point and it was determined that they should have equivalent services available to them.

Thad Hall – The group was reminded that we are tasked with looking at this issue from the voter perspective and what the voters want.

Perspective: Election Official

Election Officials Strike Back

- Registration – Election Officials need to get everything they need from the registration form the first time. Need a good address and failure notice.
- Ballot Marking – Needs to eliminate voter errors. Needs to be usable. Needs to be fully auditable.
- Needs to follow state laws.
- Ballots need to be fully separatable (separate the ballot from the envelope).

Small Group

- Registration - merge data
- Efficient way of getting ballots out to voters
- Track and see that voters obtained ballot

Team America

- Overarching integration with existing systems
- Traceability of data throughout system
- Local election rules being integrated into systems
- Did voter actually get ballot? = traceability

Perspective: Outside Observer

- Thad Hall – It was said that outside observers should be able to do whatever current laws allow now. Data gathering, etc.
- We need to make sure data is correct!
- Lowell Finley - Generate and secure as much audit information as possible. We need detailed audit files.
- Thad Hall – It was said that we needed a third party auditing firm like Price Waterhouse Coopers. Lowell Finley – It was also stated that we need someone who knows elections who has already does this like Doug Jones for example. Lowell Finley – It was also suggested that we need international observers who know US elections. They need as much access to the system as possible.
- We need to protect the privacy of the voter from the observers. We don't want to threaten the privacy of voters.
- Veronica Degraffenreid – One election official had issues with observers and the need to provide information during the busy election process. Concerns were expressed regarding teams of observers potentially coming into state / county election offices. The official did not want observers “mucking up the process” of tabulation and reporting. Observers are fine if they are there to truly observe and do not get in the way. The election official absolutely agrees with access to data by the auditors but is not in favor of people observing the process and “getting in the way”.
- Thad Hall - Differentiation between an observer and an auditor was brought up. The auditor observes the system level (including the data) and the observer observe the human level. It is necessary to observe what the system is doing as well as what the people are doing.
- Lowell Finley – It was said that observers need to see what is on the screen of the tabulation and reporting system. One suggestion that is currently in use in some jurisdictions is to have a second monitor plugged in to the tabulation system and have it wired in to another room where the observers are. He said it is possible to do this without “mucking up the process.”
- Alan Sherman – It was stated that people need to be qualified to have access to this process. Many in the group would like to see a pre-qualification process for these individuals.

- People in the group kept bringing up the reminder that we need to follow state law(s). Lowell Finley - One election official said state law does not matter with regard to this demonstration project and we must do as much observing and auditing as possible.

Perspective: Saboteur

Team America

- Registration Process: flood with false information, distribute incorrect registration credentials. Phishing
- Provide incorrect instructions, Phishing
- Mismarking ballots
- Family voting. Elderly and voters with disabilities – collecting ballots for people and remarking
- Ballot misdirection
- Transcription editing
- Certifying incorrect results
- Trojan attack
- Logic & Accuracy (L&A) Testing

Election Officials Strike Back

- Dishonest election officials
- Social engineering
- Jeremy Epstein - A paper discussing threat attack vectors that is currently posted on the USENIX website was mentioned as a possible resource.
- Cyrus Walker – One person suggested more people value their vote than their money when their vote/freedom has been taken away which is why this is a sensitive area more so than other information technology issues.
- Veronica Degraffenreid – An election official stated that most voter fraud – what little actual voter fraud there is – is done with absentee voting. Voter ID is expensive but it was said that legislators are willing to do this to protect integrity of the vote.
- Cyrus Walker – A discussion ensued about cost shifting from payroll for thousands of pollworkers to Voter ID/Internet voting costs

Small Group

- Chinese government and others have spent a lot of money researching “breaking in” and doing nefarious things online / exploiting system vulnerabilities.
- Informing voters about the processing of a vote / Redirection / Mis-addressing
- Injecting additional ballots into the process.

The groups all said that most of these attacks could happen at any point in process.

Jeremy Epstein – It was said that we should assume that all voting system vendors are 100% above-board. Cyrus Walker - Vendors should be considered an “insider” as they have access to the system and they built the system so they have deep knowledge as well. Jeremy Epstein - Vendors are getting attacked in the same way CitiBank and Google are. Attacking the vendor systems is much more cost-effective than attacking the individual counties and states. The group agreed with this.

Saboteurs will not attack pilot project/demo system. There is a disincentive to do this as then Internet voting will never go live. They will let the demonstration project go live and they will want it to be successful so that it will go live “for real” and they can attack then.

Cyrus Walker: Maximum impact and minimum exposure are the main items to accomplish by the saboteur. The most dangerous person is the insider as they have access – and these insiders are election officials and vendors. We cannot ignore them. An insider is more dangerous than an external hacker as they have knowledge of the system and access to it.

Thad Hall – It was asked why people conduct voter fraud. We need to look at their motivation. Some people do it because of local issues. Jeremy’s students, for example, – and others – will just do it for fun. Alan Sherman - Some people want to affect the outcome and have people know they did it while others may want secrecy. After group discussion, the group determined motivation can be fun, publicity, to impact income, anonymity.

Cyberterrorism is a real thing. We can’t control the intent or motivation. We can only focus on what the risks are and guarding against them. Motivation just does not matter said the group.

Alan Sherman - It depends on whether human intervention is part of the process. A human has intelligence and can determine if there as an issue – for example in voter registration, they can “eyeball” the registrations. We need to look at the degree of human intervention in each of these areas.

Risks Discussion

There was a discussion of sending in tons of manual voter registrations right at deadline as a type of denial of service of attack. These attacks are very similar.

Thad Hall – It was suggested that we can solve the ballot transition time issue by doing kiosk voting so the ballot gets printed and is also sent electronically so that there are two paths for cross-checking

Cyrus Walker – You can not ignore the coding of the system. That is typically a place that gets ignored until after the fact. We really need to be focused on that. Software architecture risks are huge. Jim Ott - Testing of systems through the VSTLs was

discussed. Vendors pay a lot of money for that. It was said that the VSTLs have mitigated a lot of risks.

Cyrus Walker – It was also said vendors don't look at security until after system is built typically and then it is an "add-on" when security should be part of the system from the ground up.. Kudos to VSTLs, but vendor systems need to do a better job focusing on security.

Jeremy Epstein – The problem with the current VSTL system is it only affords testing and approval at a single time. Cyrus Walker – Others said we need to do more testing and testing of dynamic files.

Lowell Finley – It was said that given the short time we may want people to focus on what we think are the most risky parts of the system. The group agreed and this was the direction we were going to anyway.

Jeremy Epstein – It was argued that we can't do this until we define the architecture. Without having an idea on this, all we can do is the "if and then" scenario. We need much more detail on the type of system we will use before we can go forward.

Alan Sherman - The benchmark for system testing is what's being done by the gambling authority in Nevada. There is the NY certification testing program said a VSTL representative.

Catherine Meadows - It was stated that we need to seek the same level or credibility as the gambling industry in Nevada. Laughter ensued!

Lowell Finley – One election official suggested that in any voting system the main vulnerability is between the time the ballot leaves the voter and when the ballot is locked in to the tabulation system at the voting jurisdiction – whether it is a paper or electronic system. Someone can interfere with a server on an optical scan system but there is auditing and paper ballots which serve as a tremendous disincentive.

Catherine Meadows - To further sharpen the point, it was said the threat is not so much when the ballot goes over the Internet but more the point when it actually leaves the voter's fingers and when it is actually encrypted and then decrypted on the other side. Travelling over the Internet would be somewhat safer than these points.

Jeremy Epstein – The difference between the Estonian Internet voting system and the DC Internet voting system was explained. A subtle difference in architecture – where the encryption happened - made all of the difference.

Elan Kaplan - There are tools to mitigate some of the risks. There are problems with the current systems. If not, we would not be here. There are lots of things we can do to mitigate risk and that's where we need to focus. What can we do? Lowell Finley - The definition of what the current system is is important. The average return rate in 2010 was

5.2 days if they can use military mail system. Other areas of theatre can be weeks said this study. We need to understand the current state of where we are.

Neal McBurnett – There is a desire to go back to architecture. We need to have game-changing conversations about architecture going forward. Risks depend on architecture said some of the participants.

Alan Sherman – It was asked where the issues are for ballot delivery and return. We need to look at this. We need to focus on military voters overseas with the most complex area being in theatre. While it makes sense to get the return rate up, we don't want to disenfranchise soldiers in theatre. Lets say everyone returns ballots on paper unless in theatre where it is done electronically. Let's bind this for the population that has the most issue with the current systems = soldiers in theatre.

Jim Ott – It was also suggested that we need to focus on the ability to decrypt ballots and to keep this function offline and limit it to those folks who can't mail back a ballot.

Whatever the systems is, when transmitting directly to the states and counties is discussed, that is a problem.

Lowell Finley: Is email return of ballots trustworthy? Does any computer scientist think we can do this? E-mail is inherently insecure and difficult to authenticate. There are so many ways to tamper with an email system.

David Carey - The point at which the voter has marked the ballot is the point that we need to back up to not just the point of encryption when ballot is cast.

Jeremy Epstein – We need to define the architecture!