January 29, 2014

**E2E VIV Project Workshop**

Susan opening comments – 8:50 am

Want to make it a groundbreaking project. Will say something new that has not been said before.

Interaction welcomed. Working lunch.

Introductions – project goals – the work

10 months in the making (this meeting)

Susan – decade with OVF/US Vote. Loves projects/getting things done.

Brian Leclair

Josh Benaloh – with Microsoft research (20 years). Involved 30 years with verifiable voting. Optimistic about this project. Chairs citizen oversight panel for mass transit agency in Seattle.

Douglas Jones – U of Iowa. Involved since ’94 with elections. Co-wrote book with Barbara Simons on elections

J. Alex Halderman – U. of MI professor. Involved with voting for 10 years. Taught course on digital democracy. Analysis of deployed electronic voting systems work done.

Michael Clarkson – GWU computer science. Moving to Cornell. Involved since 06 in voting.

Keith Instone – Toledo OH. Consultant. New to tech and security details re voting

Sunny S. – security program. Capstone program. New to voting.

Vanessa Tate – U of Melbourne.

Philip Stark – stats dept. at UC Berkeley. 27 years this month. Working on elections for many years.

Travis Wright – CMU grad student

Judy Murray

(missed several intros while seeking IT help)

Dean Logan – LA County clerk. Involved since 1996 w/ elections. Teaches at Cal State Northridge MPA program

Barbara Simons – retired from IBM research. On board of advisors of EAC. On group that prod. Serve report (w/ David Wagner)

Mark Earley – voting systems manager. Worked on vendor side for a while. Then returned to the county.

David Wagner – UC Berkeley. 10 years in voting work.

Paul McGuire

Roman Montoya – Bernalillo County, NM. 14 years of elections admin in NM.

Duncan Buell – comp sci prof at U of S Carolina. Formerly worked on NSA work. Began voting work in 2004 due to software issues.

David Jefferson on Skype line

2 others on Skype line – Aggelos and Peter

**Overview**

All are invited/expected to talk.

Susan’s intro – Duncan, Josh, David Wagner, Dana Chisnell, Candice, et al. began in March to discuss this.

Proposal arose. Stalemate in which election officials and comp scientists want diff things

Desire to create specifications, but there are other goals

We have a great opportunity here. Breaking a stalemate begins with us. Knock down divisions

Concern that this project is presented in a predestined way. Susan says this is not so. Not predecided. Not the case and no one here would let that be the case.

Concern whether we need to do things in a specific way. No, we don’t need to. Switching gears is fine. Creativity and breaking the mold is exciting opportunity.

Bottom line: we need to create something today. Could take all day/night.

11 months in the making, esp. all this month

Time was left for writing, reviewing, deliverables. We can make it more (videos, primer); it’s up to us for output and add-ons. Wide open for specs

This takes resources above and beyond just text. But it makes a diff re whom uses our work

We want an accessible output

We have breakout rooms (4) for smaller discussions. Use them

**Project Goals/Objectives – Susan**

This is what we signed a contract for

1. Produce a written report; a deliverable.

Adam Ambrogi – worked at senate rules; now at democracy fund. While at senate rules, he worked on voting reform, especially overseas & military. Made MOVE Act happen. He was excited about this project when proposed by Susan

Adam will be at Summit and will discuss this project from a policy perspective.

Adam and his boss completely vetted project with Susan; e.g., what happens if this doesn’t work?

Susan is optimistic. Adam and his boss are aware that this may not work out.

Susan – with the right people backing us, good things will happen. The unexpected may happen, too.

[get list from Susan to fill in any gaps below]

1. A whole product solution: looking at every aspect of makes a system. Don’t get bogged down by the word “product.”
2. Present the product
3. Framework for a secure, end-to-end voting
4. Identify the path to get the second and \_\_\_\_\_
5. Inform public of the \_\_\_

[10 minutes here for discussion]

Barbara – the focus of the meeting is E2E, but…can we look to commercially avail voting systems that are not E2E? Including in a review more than just E2E systems.

Susan: we’d need to include a realistic scope.

Duncan: the focus should be E2E

Susan: We are trying to find an E2E way to do Internet voting. For the purpose of this project, E2E is the property of an election with 2 main aspects: first, a voter can check if their ballot is cast as intended. Second, the votes can be tallied correctly and fully.

?: goal is to have an election that provides convincing evidence that the outcome is right. This is an ingredient in that, but is not sufficient/necessary. Duncan is in agreement.

Josh: missing part is “E2E verifiable.” Cryptographic, post-election monitoring, et al. need to make it as publically verifiable as possible. Wonders if E2E is misleading as is. E2E-V, actually.

Douglas: it’s great to see that my vote is up there…and I’d like to know my vote was counted, but I need to know that the outcome is right. E2E doesn’t prove that it was right outcome.

Josh: it’s all about trust; limit trust; move trust away from where it is now. Make it publically verifiable.

Verify that we have the correct outcome – what does this mean? People may not vote the way they mean to vote. 2 criteria tries to capture this as well as we can. Recorded as intended and then what is the mathematic tally?

Susan: there will be a whole segment about E2E later, too

?: it’s all about trust. Are contractors trustworthy? Not always. To date there are no solutions in the marketplace.

Candice: friendly debate on line re what systems should be capstone reviewed. Knowing the vendors, if any of the systems claiming to be E2E would complain that they are not counted as such.

Any system that claims to be E2E will be discussed by this project. Goal is to be all-inclusive in our analysis.

Vendor systems may be proprietary and not worth examining; needs to be explained by us why we’re dismissing them.

Duncan: put burden of proof on vendors as to why they are E2E.

Candice: lay out criteria for optimal systems when dismissing those that don’t make the cut.

Barbara: re verifiability of elections, that’s diff than E2E. Do we not look at a system that claims to be verifiable, but not E2E? E2E is a means to an end. Verifiability is the top issue. We must define it to get there.

Susan: this deserves ongoing conversation today.

?: the term E2E derived from a phone call and was agreed upon by the group. Auditability was the runner-up term.

Josh: we agreed on “open audits” but E2E won out b/c it was already being used by some.

Susan: we may come out of this with a different name. E2E is used a lot. Should we come up with a different name for our new product?

**Local Election Official Output Tammy**

Several local EO are here. No state EO

EO deal w/ voters face to face

Tammy is optimistic about this project

EO have been frustrated w/ us. We have been frustrated, too.

Voters are asking for certain services. EO may not be able to provide these

Tammy worked w/ Ben Ginsburg and Bob Bauer on commission, non-partisan

3 commissioners came from private sector/business and said that EO need to serve the customer

Our int’l voters are demanding of us

EO here will share their perspectives:

Roman Montoya: NM got rid of touchscreen voting. Democracy live is willing to help w/ online balloting. Not ideal, though, with 1000s of paper ballots to then tally

NM legislators would need to approve any elections changes and Roman says this would be tough

Susan: what feedback from voters? What problems are we solving?

Roman: very little feedback. Mostly from military overseas, not citizens. 90% military. They are the ones who provide feedback

Tammy: how many UOCAVA ballots are mailed out? Roman says 10,000 last election. Tammy does 8,000. Takes a lot of work to correctly tally UOCAVA ballots. Opportunity for error is introduced.

Roman: privacy concerns re voters emailing attachments instead of following the proper way

Tammy: voters don’t care about privacy as long as their ballot is counted properly. Better than having it thrown out by the EO. We shouldn’t have to position our voters to have to make this choice.

Philip: voter shouldn’t be allowed to waive it

Tammy: whether they do or don’t waive it, there is always possibility of coercion, of payment for voting a certain way.

Philip: there are other big problems, too

Tammy: how do we minimize problems? How do we stay aware of problems?

David Jefferson: vote buying/selling is a concern

David Wagner: how much are the costs? Who are the customers? Do they want to vote in local/state races or just federal?

Tammy: some overseas voters are not allowed to vote in local elections. Otherwise, return rates are much lower for local races among citizens, but military is concerned w/ local

Mark Earley: where the demand is – return rate is “good.” Democracy Live has been used; some come via mail, some via fax.

Email returns are wanted and being looked into. Legislature, not voters, is pushing for change

Fax isn’t perfect solution; vulnerability (coercion suspicion). There is demand for fax ballots, but it’s a flawed “solution”

Looking at deploying solution with bar code. This helps with cross-checking.

Candice: 2 EO have to be present in Cuyahoga County, OH

Tammy: this is common

Mark: trying to find a better solution than what is currently used. Needs to be secured and verifiable.

Need to justify why you’re deploying something for a small group and need to make it cost-effective.

Ron: questions to be answered in later segment

Dean: proactive approach here today. We’ve been reacting to 2000 and 2004 problems. Time to move ahead.

Talking about a fixed population, remote voters. Problems need to be addressed for remote voters. There are barriers to usability.

Goal is to ID what should be gold standard. How can we evaluation what reaches that standard?

What are the interest levels of remote voters? Hard to quantify. Military voters care about local elections. Don’t always get access to vote in local elections.

Feedback comes in from social media, which is helpful. This real-time usage helps EO work on problems quickly.

Elections world tends to look to voters to adapt to the systems in place. Should be the reverse.

Policy questions should be discussed today. We need to build a system that works for the next generation of voters

Lois Neuman (Rockville, MD): would like to see us be more progressive in elections.

Voting on handheld is a goal.

7 points:

1. Turnout – voters aren’t familiar w/ issues or candidates (need to be informed)
2. Database – educate EOs
3. Equipment – Diebold touchscreens are very old and breaking down. Make it easy to move! iPads would great, although they don’t work well with the old printers. Vans are needed to transport Diebolds
4. Duplications – time-consuming process w/ many people reviewing them
5. Proactive and progressive – how prog. is the community willing to be? Lois has checked w/ city atty.
6. Cost – a monstrous issue. Rockville has kept costs down, and training costs, which are labor intensive. Domino effect of costs
7. Best practices – what is the goal? What delivery of service can we achieve?

[mini networking break, 10:40 – 10:55]

**Keith Instone – Usability**

Physical usability and emotional experience usability – 2 types

Interested in hearing feedback from people re their experience

Candice (Cleveland/Cuyahoga County, OH): voters and EO both have diff experiences and diff needs

When we meet 1 set of needs, we don’t meet the other.

Mark Earley: deployability vs. usability

Barbara: audits to be conducted

Duncan: experience w/ poll manager who couldn’t use a cell phone if problems arose

146 seconds to sign Duncan in one time (in affluent precinct). System needs to be simple.

Roman: poll workers are being trained to use newer equipment and to service overseas voters

59 seconds for their county process times.

Dean: usability needs to be part of the policy discussion

Paper and tech processes are being used in tandem (not efficient)

Susan: if you have to teach a voter to use a system, any system, it’s a disaster

Keith: any time there’s a transition to a new voting technology, people are thrown for a loop

Voters complain about transitions, any new changes

Lois: speaking in defense of poll workers. It’s amazing they do as well as they do under the circumstances. Difficult job in a complex environment. She is grateful for poll workers

Training has been increased in Rockville, not before each election

They’ve created checklists (Montgomery County), inventory lists.

Early voting complicates things as well.

Can we streamline? Lighter equipment to set up easier and faster?

Tammy: since most UOCAVA voters will be accessing this electronically, we need a variety of languages in the system. Whatever we do, we need to give the voters a usable format. More info on candidates?

Make sure voters have available way to know this exists? Via OVF, FVAP, etc. How will voters be made aware of this?

If we’re starting from scratch, we need to ensure a navigable process

Ron: how do you present a voter with options? How to handle usability of optional steps?

David Wagner: focus is on security. Re: cryptographic E2E, he is concerned with usability and verification routine. Voters may not understand or trust this process. How can voters know that the system is secure?

Will the cryptographic E2E be viable? David thinks they may not work.

Josh: give voters additional options, but everything can look to voters like what they are comfortable with.

Let voters check the accuracy of their submission.

Not as pessimistic as David Wagner

Duncan: absentee votes are counted at diff times in diff jurisdictions. Not everyone counts absentee votes as “cast” – they wait until later

Mark Earley: trust issue among voters re: online voting and being able to verify it

Dean: they provide ability for voters to check and see if their vote was counted (provisional ballots too)

This gives voters confidence in their vote

Josh: this is a good option and it’s okay that not a lot of voters use it; it instills confidence in voters

Douglas: voters need to understand crypto enough to verify for themselves that their vote has been counted

?: Takoma Park has used scantegrity system

Candidates should be verifying first, and then the community eventually follows suit

David Wagner: if you can fool people into thinking they’re verified when they’re not, it’s a problem

Poorvi: a fully electronic scheme has all kinds of bugs b/c voters are not able to encrypt

Ron: complex tech. behind the scenes w/ voting systems

Voters and EO may have to go through steps, which voters might not understand, but it’s important

Execution is more imp than understanding

Duncan: it has to be something where you can check that they’ve followed directions

Richland county data has shown errors that cost votes from being counted

David Jefferson: not following protocols is more a problem of leadership and not of the people who work for them.

Dean Logan: we need good data and an idea of environmental conditions

David Wagner: how well do telephone-based systems work? Is it possible to make them usable for overseas voters?

Duncan: absentee voting takes place over a long period of time, which complicates usability. It’s a 45-day process, not a 15-minute one

Candice: the reason behind the law isn’t explained. This means the EOs aren’t invested. The understanding needs to be communicated for EOs to follow the mission

She is worried about security and the ability to fool voters, particularly given the voting debacle in OH that ruined OH’s reputation

Keith: CA has contemplated allowing audits to take place after the canvas period. What about the same for overseas voting? If enough votes come back to alter the outcome, then you count the votes

Roman: NM does this to an extent

Dean: this happens with recounts

Duncan: only once we improve the process and verify votes can we ask for policy change

Judy: diversity creates usability issues

Ron: there has to be a diff calendar involved

Has to be a complaint process if voters see problems with their vote

**Josh (w/ Ron) – Basic Election System Requirements 11:37**

1. Tally is accurate (or verifiably accurate)
2. Votes are private (or anonymous)
3. Coercion is difficult
4. Voting isn’t onerous

Systems meeting all basic requirements

Remote systems? None

In-person systems? None

Tammy: in-person voting in a single day is onerous

Dean: hard to get data on coercion; preventing people from voting is most sig coercion today

David Wagner: “good enough” needs to be lower standard for overseas voting. Can’t set bar too high right now

Douglas: certain older types of coercion is still in vogue

Electronic voting isn’t immune to coercion

David Jefferson: vote buying and selling (rather than coercion) should be discussed

E2E Verifiable Election Systems – Josh

Allows voters to track their sealed votes [these points are on Josh’s PowerPoint]

Code Voting

Enhance privacy of remote voting systems by sending individualized selection codes to voters via an alternate channel

Voters enter appropriate codes to make their selections

David Wagner: code voting is a waste of time. Josh agrees

Postal Voting Systems

Tally is accurate? No

Votes are private? Maybe

Coercion is difficult? No

Voting isn’t onerous? No

Duncan: what happens if a large number of voters claim their votes weren’t stored securely?

If votes were changed, then a recount is needed when an election is challenged

Scantegrity provides evidence if a voter has been cheated

Douglas: design a system that convinces the population of security

Ron: E2E systems have property that ballots are electronic in nature and posted on publically accessible website

1. Voters can check their vote there
2. EOs can verify tally

We need procedure if/when votes are not present.

What if the tally is wrong? This is easily handled. Normally, it’s clear what the tally should be and this can be reconstructed easily.

Roman: your vote needs to be tied back to you. This means a voter needs to be able to access their vote somehow.

Josh: but voters can’t be allowed to access the content of their vote. The EO should be able to access the content.

Ron: your vote is no longer plain text when it’s on the website. Encrypto techs can access it, however.

Voter privacy is not absolute. Voters may feel coerced b/c they know their vote is encrypted and can be accessed by the EO

Barbara: there needs to be a way to ensure there is no ballot box stuffing

Josh: in most of Europe, voting is a private matter. In US, we need to know who voted to have integrity.

Database of posted votes can have names/an ID for people to check (transparency)

Douglas: in Europe, list of voters is knowable. But countries don’t adhere to this

Ron: a separate tally of remote voters?

Tammy: what about 99.8% of voters who wouldn’t be able to check their votes like overseas voters can?

David Wagner: pragmatics about workable E2E? Where do we stand from research to product development?

Ron: 15 years away from having the technology

David Wagner:

Research now / 0-5 years of research / ???

Product development:

Under $1 million / $1-$10 million / $10 million+ ?

Travis: can we verify is overseas registered voters didn’t vote in order to determine that their vote wasn’t stolen?

Ron: voting or not voting is not private

Aggelos: possible for a core system to be less usable and offer more security properties

Flexibility and tradeoffs. If the system is flexible enough, the interface can change the voter experience

Duncan: some users don’t want their ballots as unsecurable as that

Douglas: unacceptable to let users opt out of certain properties

Josh: universal verifiability doesn’t need to be accessible to every voter

Various interest groups can do this

Ron: combine E2E to Internet voting? Big project

Vanessa: this is a complicated process

[lunch break at 12:24 pm]

**David Wagner**

Come up with a direction re: how to serve mil and overseas voters

In-scope solutions, creative new approaches, worth our time to institute

Ron: Proxy voting

Roman: 2 types of overseas voters, one is more office-like personnel and second is military w/ very limited ‘net access (1 hr. per wk.)

Josh: Portable micro-polls (at embassies, consulates, mil bases, mil ships, etc.)

Need 2 minimally trained observers and a laptop

David W: this is not a new approach

This is costly

Not all overseas citizens live near an embassy/consulate

Tammy: who provides the equipment?

Josh says verifiability is an issue.

Alex:

* “Null solution” – overseas voters won’t be accepted, but early voting will be accepted

No taxes would be good, since US is only developed nation that taxes its overseas citizens

* Null solution 2 – fly voters home to vote; may be cheaper than the alternative
* Null solution 3 – allow voting at the embassy

Doug

1. Proxy voting in which you sign over your voting card to someone

Nursing home abuses of this system abound

This is not legal

1. UOCAVA voters share new congressional districts (there are 2). Then everyone gets the same ballot style

Congressman would work toward no taxes for overseas citizens

Vanessa:

Voting by mail; this would marry cryptography with Internet-to-mail voting.

Voter would be able to verify if their vote was recorded properly

Vanessa says there are still issues to resolve with this idea

Philip:

Extend calendar period for UOCAVA voters

A $10 million problem to solve nationwide, not a $100 million problem

Or…liberate the counties from the responsibility of mailing out all the ballots

Barbara:

Also advocates extending the calendar for mail-in ballots

Voters have 1-2 weeks to get their ballot in, as long as it’s before Election Day.

Filip:

Code voting

Has limitations, but can work similar to how we use credit cards to buy on line

Combine it with paper and scratch-offs

Optional privacy, if you destroy your ballot later

Ron: what is the level of documentation? Filip has evidence he can share

David Wagner

1. Phone confirmation: finalize your ballot on line; then receive a phone call to confirm and cast your ballot.

Server (run by county or state) receives these ballots and sends them to an independent agency. That agency then calls you for confirmation. 2-channel solution with double-confirmation

Alex: there are difficulties with the multi-channel aspect. David W. conceded that fact.

1. Poor Man’s E2E: how to do it w/o cryptography to save on the high costs…

I vote, I get a tracking #, and the vote is shown next to that # (w/o my name)

EOs have to keep the # secret (this is a fault)

2 or 3 tracking #s might be necessary, one federal and one state

This is based on a lot of trust by overseas voters of their EOs

Susan:

Simplify – in favor of turnout and to secure elections

This plan allows overseas voting indefinitely. We never lose it.

Start with federal elections only. 1 office per state supports it. DHS would administer it.

1 ballot for all would be used

This could eventually be used with E2E

Mark: Similar plan to Susan’s, but also allocate funds to getting the ballots back to the EOs

A centralized plan

David W.: Reactions? Technical solutions? Policy solutions?

Roman: centralization a great idea; however, there are voters abroad who do want to vote local, too.

Susan: makes sense that an EO would shoot down centralization for this reason

Tammy: OH would sign on quickly to centralization

She wants anyone eligible to have full access to any jurisdiction they want to vote for

Susan: only gets federal ballot, no local ballots. This is a county decision. This is b/c she is overseas indefinitely, not for a finite time period.

Poorvi: has reservations about all above ideas; interested in discussing all further

[break from 1:45 – 2:05 pm]

**2 Groups Break-out Session – LEOs and Technicals**

[2:05 – 3:30 pm]

Reconvene 2 Groups @ 3:30 pm

**Dean: Defining the End User in Terms of the Voter**

End user = remote voters in general w/ 6 or 7 categories:

* Military deployment
* Civilian overseas deployment
* Students
* Missionary service
* First responders
* Short-term unscheduled deployment
* Short-term in-country unscheduled deployment away from your precinct

Identified policy concerns…

* Segregating a class of voters
* Voting period
* Lack of uniformity of canvassing
* Auditability of voting
* Ease of verifying at voter level
* Voter registration barriers
* Military deployment and reg. issues

Policy ideas:

* Multiple modes of issuing ballots and collecting them
* Pre-marking sample ballots (by the voter, not the EO)
* Registration barrier: more automatic reg. model and interstate data matching

Usability concerns:

* Lack of options and tech concerns
* Paper based solutions

Usability ideas:

* Online marking tools
* 2D bar codes
* Uniform ballot standards

[Notes from Dean inserted below:]

Break Out Discussion (LEO/Policy/Usability)  
>January 29, 2014 -- E2E VIV Workshop  
  
>Define the end user: Remote Voters (broad definition)  
>-- Military Deployment (short/long term) (in country/overseas)  
>-- Civilian Overseas Deployment (short/long term)  
>-- Students (in country/overseas)  
>-- Missionary Service  
>-- First Responders  
>-- Short term/Unscheduled Deployment  
>-- Short term/Unscheduled Local Absence from assigned location

>Policy Concerns: isolation/segregation; relatively short/complete voting period; lack of uniformity of canvass periods and scope; audit ability (voter level) of paperless systems; ease of ability (voter level) to verify using cryptography; registration barriers (first time voters, etc.); voter authentication limitations/instability (i.e., signature match); single points of vulnerability (i.e., local vs. state responsibility)

>Policy Ideas: authorization of multi-modes (including electronic/paperless) of issuing, marking and submitting ballots; protocols based on post-certification verification and results modification; pre-marked sample ballots options; automatic registration models; interstate data matching; enable passport validation for voter registration/voting purposes.

>Usability Concerns: lack of options (technical access limitations); access and transit issues associated with limitation to exclusively paper-based solutions

>Usability Ideas: Democracy Live/Everyone Counts model of online marking/2D barcodes; uniform ballot design standards; common data formats; COTS adaptability.

Josh: short voting period?

Dean: needs to be a defined period from the voter perspective

Ron: voter reg./credentials. How do voters get credentials?

Dean: it’s an issue that needs to be discussed. Signature match is current way of ID’ing voters. Non-transferrable credentials are needed.

Tammy: passport can be used in combination w/ another form of ID. Doesn’t have address, so it proves citizenship, but can’t be used alone for voting in most states.

Susan: passport is a federal document and most states don’t accept it b/c it’s hard to work with.

Duncan: SC allows passports and it’s one of the most voter suppressing states

Dean: states will create a random ID# if you don’t fill in last 4 of your SS# or your driver’s license #. Passports aren’t accepted.

Dean: what would it take to get the availability to verify passport #s?

Josh: embedded chip maybe can be used to verify ownership and location.

**Tech Group – Duncan**

“Auth.” – untrusted computer – untrusted network – untrusted central systems

Corruption (evidence) vs. disruption (e.g., denial of service)

E2E-V handles most of this very well and detects existence of some corruption and disruption

How do you start this process?

Duncan says we’re close to coming up with something that lists/specifies what the system should look like

Credential/verification = a main issue

David W.: more ideas from mini mini breakout

1. Ballots are printed & mailed. Reduces burden of verification to make scheme more usable

Codes underneath scratch-off used with app on smartphone

Goods of code voting w/o negatives

One or the other could be tampered w/ but not both (phone and paper ballot)

1. Phone verification
2. Designated verification
3. Social voting

Barbara: 2 channels are necessary

Douglas: Estonia’s national ID card system works well

Tammy: if 2 channels are a requirement, then what do voters do who only have 1 channel?

Poorvi: 1 channel could be postal system (paper)

Josh: do we think a paper channel is equivalent from voter to EO and vice versa?

David J.: why even consider the paper ballot as a channel from the voter to the LEO? No better than the current absentee ballot in use, right?

Duncan: we need to look at what happens if there are 2 offices – 1 providing credentials and one sending ballots

Tammy: we want to ensure the security of systems in place. Simple answers are sometimes the best solutions

Susan: cautions against tossing out ideas just because there may be some bugs in it

Tammy: paper has risks; “ballot leakage” has security risks. The various points where ballots could be lost along the way.

[break 4:15 - 4:34 pm]

**Candice – CMU Capstone Project**

**“Comparative Assessment of Extant Claimed E2E or Remote Systems”**

Goals:

1. Analytic template – headings and Qs to ask
2. Systems to include and tag – prime foci

Intros of CMU grad students

Not comp sci students. Systems mgmt. and orientation mgmt.

Not developers or working w/ source code

Security / [usability / accessibility] / auditability

Sources:

Research papers 🡪 use templates

How many collaborators req to bring down system – Brennan Center report

NIST Risk Assessment (mail vs. elec)

Whom do we need to trust (and how many) to be assured accurate tally? What’s evidence?

Visibility – to what extent studied?

Accessibility

[unreadable white board notes]

Resiliency/recover

Lifespan of system

Threat \_\_\_\_\_ changes constantly

Resistance to malware host and office server

Timeline of election and election calendar

Prevention and detection and attribution 🡪 correctable malware

Timeline of election and election calendar

Prevention and detection and attribution 🡪 correctability

Scalability – 2,000 voters vs. 2 million voters

Physical emergencies and jurisdiction’s ability to withstand it

What is the threat model used in each? National, state? What level of attack?

Goal of report is to begin discussion of further objectives and discussion. Their CMU deliverable will be the first such report.

Susan: caution against NDA

Comparative analyses being done is a concern to vendors

Vendors worry comp sec experts want to steal their code and build from it. Candice says this is laughable.

Josh: refuse NDAs completely

Paul M.: NDAs are not feasible anyway

Poorvi: Open source code available? Not sure how to use it, but good to know

Barbara: do you want to distinguish b/t public and private elections?

Tammy: sufficient # of voters checking ballots?

Benchmark for # of voters \_\_\_ check?

Any issues arise from checks/complaints?

Vendor dependence/independence from long-term tech help?

Lois: size of equipment/storage consistency; ease of use

[unreadable white board notes]

Testing - # of voters; LEO’s experience

Integration/merger of results w/ existing in-person/EMS

Tammy: usability of actual stream of characters verified? Alpha numeric? Caps vs. lower-case

Ron: strings – research for usability and variability

Douglas: compatibility with state law – no marked ballots

Ron: suggestion of mailing out PDFs (not discussed further here).

Susan: has anyone recommended models or price structure? Other kinds of software (database) info would be helpful, too

Candice: Gartner has been contacted

Douglas: patent context and IP restrictions

Candice: to send out summary and will ask for further suggestions and to prioritize everything that has made the list so far

What systems should be put on the list?

* vendors need to be investigated – Helios, remotegrity, civitas, pretty good democracy, Canadian system, Juan gilbert system (not credible), Australian state of Victoria system, starvote, votebox, veriscan, new south wales system
* Estonia, Norway, Reis, French govt (seidl)

Vanessa: discussion of different Australian systems

Categories of deployed systems vs. academic systems

David J.: put out a call for systems to self-nominate

Candice: report will be for OVF, the client, inclusive of the entire E2E group

Wants a technical report as well as a report written in less technical vernacular

Required to finish first draft by 3rd week of April

Susan will visit March 3 for first visit. Final pres. will be in May

The biblio has been started.

Helios has a vast number of papers

Judy: added a new folder in the Dropbox for relevant docs/files

Vanessa: concern that the scope of numbers of projects and numbers of tasks may be too great for 1 capstone team

Susan: you’re the consultants and OVF will accept your word about your abilities and schedule.

Candice: Lori faith Kramer is a prof at CMU

Josh proposal to Kramer re usability for a study one of her teams could do

Teams/groups will be picked and work will begin

Josh: Helios and remotegrity could be picked. Or maybe other systems

Candice: Proposed ranking to be sent of projects for capstone to work on

Susan: a lot of ground to cover. This project will be fascinating and is a good start to sink our teeth into

Dan Wallach (who will be at Summit) suggested a technical writer to work on the project; funds are set aside for this position.

Josh will ask the current writer working on the starvote project, who may be available now

**Susan: discussion about Summit**

Key note speaker (Pat Hollern) is snowed in due to snow in Florida.

Tammy will be new key note speaker

60 sign-ups in last day or 2

Rep. John Conyers will be pm key note speaker

NBC and voice of America will be there

January 31, 2014

**Workshop Day 2**

8:57 am, Susan intro

Andrew Regenscheid, mathematician at NIST, is here today

Dan Wallach, Rice U. is here today – working w/ Dana on STARVote Project

Bingbing Hou is here today – part of capstone team

Dana DeBeauvoir is here today – LEO, Travis County, TX

Today’s Plan

Goals

Together

Breakouts (which rooms?)

Summit Debrief

Feedback: our own

Philip: feedback about whether voter understanding is needed of E2E. Some people need to understand it, while others don’t need to in order to understand it.

Dichotomy b/t understanding vs. trust

Tammy: some people as what’s the diff b/t trusting their election administrator vs. trusting the technology?

Josh: voters say they’re being asked to replace their trust in election admins w/ trust in crypto.

Dean: re: transparency, voters need to understand it to be able to trust it.

Susan: seeking someone here to take charge of E2E trust issue. Philip asked to do so, but has no time.

We now own this problem. Voters see it as Voodoo. Voters want to see it to believe it and trust it.

Philip has slides to send to Susan.

Josh: we need to come up with pedagogical tools to get the message across

Feedback re: Josh’s card trick demonstration. Tammy liked it, Susan liked it. Some concern from others about how it looks like magic, charlatanism. Bad connotation.

Philip: card trick is great way to convince voters their vote is read, but not great in other ways.

Dana: we need to find a way to explain this. Soundbites. Sentence or 2. 2 or 3 levels of explanation. Not a fan of card trick metaphor. 80% confidence level in the process. Can we come up with something better? Marketing piece is no small thing to ignore.

Susan: we could have couple of pages of talking points. Legit to say we don’t yet know how to explain E2E, but we have 1.5 yrs. to work on it.

We threw ourselves in the bathtub of our project and had to fight our words. Kind of skipped to the end w/o yet having the middle steps figured out.

Message issues will linger for now.

Ron: Scantegrity was good, had helpful explanations for voters included.

Maybe we can do a similar system with paper return.

Susan: we need to drive the conversation, rather than react to it. E2E is now doing this.

Should we have a second website for this project? Or use OVF? We could move it if needed.

Duncan: branding of OVF is good for this project

Mark: down the line we’ll need partnerships for the deployment; not just via OVF site

Susan: certain partnerships are for the end, when we have something concrete to deploy.

Other feedback?

People learned something. They were fascinated by Summit.

Suggestions for E2E Comms./PR/Messaging

Vanessa: vendors will be right on top of perceived advocacy of E2E. We won’t have 1.5 years to explain what we have.

Susan: was cornered by ES&S (vendor) to get a jump on E2E

Should we think of a diff name eventually?

Group says we can’t patent/trademark the name. it’s a term in the lexicon now.

We might end up w/ new name when it becomes final

Dean: we shouldn’t compete with vendors. We win by doing our work on our own.

Susan: what threatens vendors more is us not caring what they do.

Philip: E2E-V is the key name here. The V is crucial, as Josh pointed out Wed.

Josh: we’re publically auditable, universally auditable, and verifiable

Wed. Day 1 Workshop

What worked?

What should we continue?

David W.: breakouts were AWESOME!!! Very excited about the work done and ideas developed in breakout. Suggests more breakouts today and would like to be put in charge today. (“elect me dictator”)

1. We talked about multi-channel schemes

* 2 devices
* Paper device

1. One-channel

* Voice
* Video

1. Incremental

* Ballot duplication
* Late deadlines

1. E2E

Josh: the matrix is imp. What’s there? What combo of properties have been hit upon? What targets should we shoot for? What’s valuable? An Internet scheme that targets like Scantegrity does. Paper trail that provides trust perhaps. In 99% of elections, no one will touch the paper, but knowing it’s there makes a big difference.

Duncan: the “why?” is imp. Explain why we do what we do.

Aggelos: will miss most of meeting due to lecture for 3 hrs.

Would like to vote for code voting. It can authenticate voter at moment of voting. A nifty property that could be positive in some sense. Ballot contains the codes and ballots act as authentication for voters (2 birds w/ 1 stone).

How are the codes distributed? Aggelos says codes are mailed to voters (or sent via distribution points) and voters enter code on website. Entering the code gets you automatically authenticated.

Philip: about to mention 1 problem, but Susan tabled the negative comment.

David W.: shows list of teams and assignments for breakout session

* Tech design teams (3)
* Admin teams (2)
* Specs or voter authentication or combo of properties
* Essential infrastructure

Susan: we can’t work on policy here. We shouldn’t have to move deadlines later – it won’t happen. Goal of project is not policy.

Dean: argues in favor of discussing policy issues

Susan: why would we choose 1 thing to work on, when so much is undecided right now?

Barbara: we’re putting a lot of time/energy into a system that may not come to fruition. Isn’t policy part of the issue? We need to know what to solve to come up with a solution.

Only proposal now is technological. What if other solutions exist? We need to discuss to find that out.

David W.: let’s not spend time debating this point.

Dean: asking Susan to explain the purpose of this project before we head into breakouts

Susan: definition of the problem: our country has never defined our Internet voting system. We have offers from vendors (and from other countries) to define the problem. This project is about us defining it/solving it before someone else does. We ID it. Here is where it’s not right. Here is where it needs more work. If we’re not the ones defining it, then someone else will and our project has no purpose.

There are so many details – policy implications; what ballot return looks like. Do you disagree?

Ron: if you build a better mousetrap, people will use it.

Judy: from a poli sci perspective, there is a huge research gap re mil and overseas voters and how their handled by US.

This segment is not very engaged in the political process. Overseas voters have a very low voting turnout rate. Lack of research why this is the case. We can fill that void.

Susan: domestic segment is also a big one – people here who can’t get to the polls and are forgotten (e.g., disabled)

Ron: security issue is a key concern; adversary may manipulate the outcome

Susan: this project is a way to address that issue

Andrew: challenge is having an evaluation process to determine readiness

Hard to come up with formal testing process

Josh: could there be testing against properties, if we come up with certain properties?

Andrew: this will be extremely difficult. Evaluation procedures will be tough

Duncan: they won’t give us source code to test

Josh: we don’t need source code to determine what will be E2E-V or not

Ron: testing is needed to ensure the system is not hackable

Dean: we don’t need something each election year similar to U of M project

David W.: our time today is super precious. Urging group to begin breakout sessions ASAP.

[breakouts/lunch 10:10 am – 12:58 pm]

Tech 1 Team – Josh

Looked at very incremental approach. What can they achieve in a short time?

1999 – a CA Internet Voting Task Force (David J. was on it); it got out in front of Internet voting w/ a pathway of discreet steps:

1. Internet voting from poll sites
2. Internet voting from non-precinct/county poll sites (more flexibility)
3. Not voting from home, but from public sites (libraries, schools)
4. Vote from home via Internet

Is there a way to apply STAR Vote to this system to make it tradition w/ E2E, rather than a whole new system that people aren’t comfortable with?

Let’s do something w/ trad. paper ballot return, but with a Helios-type appl. for voters.

Flow is ~ you ask for an absentee ballot and get a Helios interface on your computer, then you print & send electronically w/ E2E verification.

Benefits of this system:

From voter POV, there’s a nice ballot marking system to use

An extension of deadlines

EOs don’t have to mark the ballots

Couldn’t figure out authentication.

Tech 2 Team David W.

Voter needs 2 devices (laptop, phone…)

If we came up w/ a scheme involving 2 devices, is worthwhile? Tammy checked and says it’s feasible.

Roman: Military in active combat have their personal phones taken away, so this complicates the 2-device issue.

Josh: you can assume multiple devices as long as there are choices (mail option is a choice)

Susan: pretty soon, all devices do all things and you won’t need 2.

How do you confirm these are 2 distinct devices? IP address?

Dual-channel banking, used in Germany, is very usable; could work here

No matter what gets created, paper system will always be the fallback. We aren’t going to replace that. We are adding TO that system.

David W.: human-to-human phone call/Skype call to your EO.

Issue w/ this is the privacy matter. What if the choice is b/t not voting or voting w/o privacy?

Tammy: LEOs will still have to provide assistance, even if system isn’t private. Main mission is to assist voters no matter what.

Douglas: system can be similar to airport security machines. The human on the LEO end need not know who the voter is (anonymous, but not private).

Dean: voter makes the decision, not the LEO.

The project can’t push privacy to the backburner.

Candice: is there going to be a video or audio record kept?

Protections at receiving end need to be in place.

Barbara: comparisons to Jim Crow US and civil rights struggles where people were murdered when trying to register to vote

People of color are nervous still about lack of privacy

David J.: doesn’t look like a scalable automated attack on privacy

Receipt can’t be taken and sold

Duncan: how is this going to be written on the front page of the Post?

Voter Auth. Team – Ron

Getting credentials to voters so they can vote on line free from online attacks

2 or more PINs given to voter (10-digit #)

PINs are set up over different channels

Each PIN has a validity # (a year or so)

Any channel may be subject to attack, hence the extra PINs.

Postal PIN, email PIN, phone channel are examples

Military voters have hard time communicating, aside from email usage

Use of multi-channeling for credential process may deem single-channel useful later on if automated attack threat is mitigated

LEO Support Group – Philip

Philip will send brief email to Susan to clarify

Infrastructure Team

What kind of system will be used? Bulletin board? Commercially avail or licensed?

What type of setup would juris. like to have?

Need a separate database server

Key question – info won’t be shareable b/t jurisdictions

What limitations are there at the county/state level?

Candice: infrastructure will be expensive. Will require more resources than currently available.

Also, manpower just won’t be available to maintain all these needed systems/databases.

There is a problem w/ antiquated laws; they’re not keeping up with 21st century processes

Susan – What’s Next?

Candice will send Capstone project work to group via a Wiki, or some other method

<Discussion among group re: goals for today and beyond.>

Ron: are discussions here confidential to the group?

Susan: basic assumption of openness. Thinks confidentially was removed officially. But w/ understanding of not sharing info.

Paul: confidentially not mentioned explicitly. 80% agreed to confidentiality.

We have a contract signed with Democracy Fund; we’re not bound to confidentiality. Project findings will be shared with DF (use right), which will publish what it sees fit.

Purpose of this exercise is to share info w/ public

Gray area in between

Douglas: none of us speaking individually is speaking for the group

No one is able to commit the group the anything or speak for the group

Susan: we’re in a formative stage, delicate stage. Ask Susan questions re: any concerns about confidentiality or potentially damaging the project.

Each of us is a caretaker of the project.

Presentation by Philip

Wallach’s Insight (D. Wallach)

The purpose of an election is to convince the loser s/he lost.

Evidence-Based Elections (PBS, D. Wagner)

Elections officials should provide convincing evidence that the outcomes are right, or admit that no such evidence is forthcoming.

What’s Convincing?

Depends on whom/what you trust – and for what.

One person’s “obviously” is another’s “seriously?”

Is there a reasonable standard of a reasonable person?

E2E

Personal verifiability: voter can verify whether her vote was cast as intended and included in the tally.

Universal verifiability…

Claim: Much Ado about orthogonal Issues

Case as intended, recorded as cast, counted…

What/whom do elections require us to trust?

Varies widely. Trust for accuracy differs from trust for anonymity

Might include:

Ourselves

Other voters

Vendors

Hardware

Softward and programmers

EOs

Pollworkers

Stats

Trust whom, for what?

Evidence about outcomes? Assured anonymity? Public confidence?

How hard is it for the trusted party to do her job?

What is the conseq of failure?

Is the trustee the potential attacker?

What failures can be recovered from?

Proposed notional goals for voting systems

1. Give convincing evidence that outcome is right
2. Be affordable, practical, maintainable, explainable
3. Robustify more than harden
4. …
5. …

[get notes from Philip or on line – he’s skimming through PowerPoint too quickly]

Tradeoffs

Group discussion on E2E-V vs. hand-to-eye verifiability

Ron: Philip is dissing E2E a little bit

Philip: basic E2E like tamper-evident seal: SI, not SSI

Can tell that something sent wrong – if there is enough…

[end topic]

David J.: we need to remain committed to saying if we cannot solve the problems. Be frank rather than risk national security or other issues.

Dana: we need to look at electronic only rather than risk leaving anything in the field w/ the paper system

Privacy issues are tough to mitigate

Susan: if this is going to involve paper, then why do this?

David W.: our baseline is electronic ballot delivery and paper ballot return. Paper ballot return is not fast enough of reliable enough. This is why we’re here.

Josh: not satisfied either with current process.

If paper is left in the field, it’s not a copy of a valid ballot

Duncan: let’s put all our eggs in one basket and see if it’s good enough

Susan: let’s not just exchange one set of problems for another

Josh: this improvement so far is minimal for voters and LEOs.

This is a scaffolding approach; build this around the current system and then remove the scaffolding when this is better than the paper approach.

Could be decided 5 years down the line when you see that you haven’t looked at paper ballots in a long time.

Douglas: agrees, if audit technique works without paper

Poorvi: paper is a nec. part of even crypto system

Susan: if you need paper to vote, it’s a problem

Josh: we’re talking about paper 1 way from the voter to the LEO

Philip:

Benefits – paper is recorded electronically immediately by LEO w/ barcode scanner

Less time and less work required

Poorvi: paper is necessary in the E2E process

Add dispute resolution property to E2E to avoid more confusion and throwing out honest elections

Lois: her city has low voter turnout, esp. among young voters

Handhelds, laptops, etc. will appeal to young voters

Need to cut out long wait times that keep people away

LEOs need proof, evidence and paper ties into this tangibility

Keep paper b/c voters and LEOs are familiar w/ it. Then gradually peel it away over time.

Josh: voter simplicity is the key

Lois: how to tell the voter it’s private?

Judy: what is being described here is not good

Please think further, think outside the box, think bigger instead of the incremental steps proposed

Barbara: there are some problems that can’t be solved. No matter how much you wish that some problems could be solved, they just can’t.

Dana: feels this is solvable

Fillip: 2nd device is best wait to maintain integrity, but it disenfranchises voters who don’t have multiple devices

Dan: You gotta trust something. Anything we might want to trust, we can come up w/ a reason why we don’t like it or trust it. This is a problem. Instead, we need to come up with a way to trust them. Work to surmount the problem.

Fraud detection process is complicated and still very flawed. Not really the bar we should/could aspire to, though.

[misc. thoughts on schedule for afternoon; 5 members are leaving at 3:00 pm; breakouts lasted until about 4:00 p.m. to conclude Day 2]