Next Steps for E2E Voting Systems

Presentation to the
NIST End-to-End Voting Workshop
Washington DC
October 14 2009

Jeremy Epstein
Senior Computer Scientist
SRI International
jeremy.epstein@sri.com
703-989-8907

Step #1: Step Back

What are the *real* requirements we're trying to meet?

- Does it matter whether voters and election officials can understand how the voting system works?
- For crypto E2E Internet voting, does it matter that end system security is an unsolved (and probably unsolvable) problem?
- Are the crypto E2E systems versatile enough to handle all the types of elections in the US, given widely varying laws?

What are the advantages in meeting requirements?

- Can crypto E2E make it easier to meet post-election audit requirements?

Step #2: Barriers to Deployment

State and local attitudes

- Given the DRE fiasco, will states and localities take on another experimental approach?
- How much easier or harder is a crypto E2E system to manage for non-technical election staff and pollworkers?

Voting system certification

- How could E2E systems be certified under today's regime?
- What modifications would be necessary to allow certification?
- What loopholes would new certification regimes introduce?

Step #3: Usability Testing

Usability for voters without disabilities

- Are voters able to understand *how* to cast the vote with a crypto E2E system?
- Are voters able to understand *why* the crypto system protects their privacy, gives security, etc?
- Are voters able to understand how to check their votes?
- In practice, do enough voters check their votes that we get the desired verification results?
- For Internet systems, do voters understand the risks of using an unsecured system to cast their vote?

Usability for voters with disabilities

- Are there unique challenges for voters with disabilities on crypto E2E systems?
- Are there changes that are needed so the crypto functions can be accessible to them?

Step #4: Security Assessments

Given that the crypto is correct:

- Can we tell the difference between a good and bad implementation?
- Are there non-crypto vulnerabilities that might allow bypassing the crypto schemes?
- Can non-technical administrators successfully set up a crypto system in a secure fashion?

Step #5: How do we get E2E all the way to the voter?

Can we make an argument about kiosk + E2E = good enough?

Or is that just a steppingstone to vote-from-home-using-a-compromised-computer?

Can we marry crypto E2E with "code voting" to get a system that allows *truly* E2E secure voting?

Questions?

Next Steps for E2E Voting Systems

Jeremy Epstein
Senior Computer Scientist
SRI International
jeremy.epstein@sri.com
703-989-8907