Independent Computations for Safe Remote Electronic Voting
(Transcript of Discussion)

Alec Yasinsac
University of South Alabama

So this is a good follow-on to the previous papers. I’ve been working on electronic voting for several years, and as a retired U.S. Marine, I voted absentee for 20 years, and having not known much about voting and the electoral process when I was voting, when I began studying the electoral process I realized how many times I sent my ballot in and it wasn’t counted, because, for example, in the military when you make a mistake you cross it out with a pencil and you initial it. Well when I did that on my ballot, that ballot went in the trashcan. Of course I had no idea. So since I’ve been involved with information security for a while, when I retired from the Marine Corps, I made this a focus of my research.

And I come at it from a perspective that’s slightly different from many of my colleagues, and as a matter of full disclosure, my objective is to find a way for military members to deliver a voted ballot electronically. My objective is not to say, “is there possibly a way”; my objective is to find a way.

The notion here is pretty foundational. From a theoretical perspective, digital verification is hard. The Halting Problem says that using one computer program to verify another computer program is folly; you can’t do that for arbitrary programs. That’s the theoretical result. More practically speaking we know that it is hard because malware is pervasive, and in fact one of the hardest problems with remote electronic voting is being able to verify that you are doing these things with code that is unflawed.

There’s a notion out there now of software attestation that would be a great thing to have for remote voting, and I’ve spent some time working on that too, but that’s a little bit further down the road. Once you can be sure that the software that’s running on that computer is the software that’s supposed to be running there, that gives you a lot more flexibility to come up with protocols that can make voting safe. Still, I well-understand the reasons why many of my colleagues don’t believe it’s possible to vote remotely over electronic media today. What I’m here to offer you is, what I think is a fundamental difference in the ability to verify these ballots at the end and to make the argument that there are practical voting systems out there today that have some of the properties that could allow this to happen in a real election. So that’s the goal of this paper today. I want to acknowledge several students, because they worked very hard, and they worked mostly independent of me: Erin Pettis, Son Le, Naquita Hunter, and Mengchu Lin. I gave them a copy of the paper, and their mentor, Terri Gilbert, and they implemented it as their senior, capstone project.
They put it together and they wrote a voting system that actually implemented all of these concepts. It’s not been used in any kind of election, but this is my fifth paper at the Security Protocols Workshop, so I know very well that you all know that the devil is in the details. It’s awfully nice to have these high level protocols that have all these properties that you can prove, but then when you actually put them in the computer and in a machine, you know, it just didn’t work out the way you thought it was going to work out. So that’s a major contribution, from my perspective, that we have a system that actually runs, and it runs with handheld devices in the Android environment with a laptop computer, and that we made these things work in the laboratory. So I appreciate the work that they did, it gives me a little bit more confidence.

Now I want to back up just a minute and talk about this notion of universal verifiability, end-to-end voting systems. This terminology is not really well understood, even by some that have been doing this for a long time. The notion here regards the three steps in the middle that are the canonical steps in the voting integrity process. Have you cast that ballot as is intended? Now I argue that from a real perspective it’s almost impossible to measure, because the intent of that voter is in that voter’s mind. It may be that a voter doesn’t have an intent that you can even describe. Maybe they voted for candidate A because they didn’t like candidate B, or because they liked candidate A’s name, or because candidate A was the first position on the ballot. We don’t know what the voter’s intentions are, so the metric that I have used is, “is it voter verifiable”, i.e. can the voter look at what they cast and in some way say, yes, that’s what I want to vote. So when they take a second look, they get a chance to be able to fix a mistake.

Now that’s a very weak form of Cast as Intended, but it’s probably, at least in my opinion, about as good as you can do. Now the real point of this slide is the difference between these two, “Recorded as Cast” and “Tallied as Recorded”. The notion of Recorded as Cast is: I have some way to be able to determine that the local elections official that I sent my ballot to actually received the ballot in the form that I intended it to be delivered. Are all the selections on the ballot that the local elections official has the same as those that I intended for them to have? Now that is far better than the system that we have in place today. The gold standard of the voting elections community, is a Precinct Count Optical Scan system where you take your ballot, and you mark your ballot, put it in an envelope (or not), and you feed it in to this machine that scans it right there. Or maybe it scans it; maybe it’s actually a shredder. It may well be that all those machines in some precincts really aren’t counting those ballots, they may be shredding the ones that are received and dumping one that is in a bin underneath that shredder into the counted pot, that could really well be what’s happening in all of those precincts throughout the United States.

So we do not have “Recorded as Cast” confidence today. While we think we have the gold standard in the United States, PCOS voting integrity system is Cast as Intended. Now I argue here that getting down to Tallied as Intended, or Tallied as Recorded and Tallied as Intended, is actually not an important