Internet Voting for UOCAVA Voters
Notes on the Relevance of European Experience

Douglas W. Jones*
Department of Computer Science
University of Iowa
Iowa City, Iowa
Email: jones@cs.uiowa.edu

Over the past decade, several European countries have flirted with and some have adopted Internet voting. In some cases, notably that of Geneva, Switzerland and the Netherlands, one of the primary motives for Internet voting was to better serve the needs of expatriate voters. In both countries, the complaints of expatriate voters were very similar to the complaints of UOCAVA voters. Too many requested postal ballots never arrived or, if they did arrive, they arrived too late to be returned in time to be counted.

There are some important differences, however, between the election environments of Europe and the United States, and these need to be understood before drawing conclusions from the european examples. I want to emphasize these differences here:

Obligations of Government and the Obligations of the Citizen

One of the first and most important differences is one of voter registration. In both Switzerland and the Netherlands, the government is obligated to track down and provide voting credentials to every citizen who is eligible to vote, and it is cause for scandal if the government fails in this obligation. Until recently, voting in the Netherlands was obligatory. This government obligation, of course, is only feasible if citizens are obligated to register their current addresses with the authorities.

Citizenship does not automatically translate to voter registration in the United States, and once registered, U.S. voters may still need to explicitly request a ballot. Voter registration is optional, and in most jurisdictions, absentee ballots are only provided on request. There are exceptions to this in states with universal or very widespread no-fault postal voting where voters may request to be put on permanent "absentee" status.

The Case of the Netherlands

The Netherlands has no tradition of use of postal voting domestically. If a voter cannot go to the polls during normal voting hours on the election day, that voter may vote by proxy. That is, the voter signs his or her voting card over to someone else. A husband who is traveling on business during the election may sign his card over to his wife, for example. Short-term expatriates, for example, those leaving the country for a brief trip, may easily use this proxy mechanism.

Of course, proxies are subject to abuse, just as postal absentee ballots are subject to abuse. Many of the abuses are very similar. In the United States, we have had scandals involving nursing-home workers voting the absentee ballots of their patients. In the Netherlands, the current limits on how many proxies a single voter may vote are the result of a very similar scandal.

Long-term expatriate voters in the Netherlands do not vote in their home jurisdiction. Instead, all expatriates vote in the jurisdiction of The Hague. This means that only one election office in all of Holland needs to handle postal absentee ballots, and it handles them for all expatriate citizens. This works, in part, because the Dutch do not combine elections the way we do. A national parliamentary election is never combined with regional elections. Furthermore, although the parties are allowed to

* supported in part by NSF grant CNS-052431 (ACCURATE)

run different party lists in different regions, they no longer do so. All members of the Dutch Parliament are elected at large, so the same ballot, listing many hundreds of candidates, is seen by every voter in the country.

In the United States, in contrast, UOCAVA voters are entitled to vote on the ballot style of their domestic home address. There are something like 7,000 distinct local election administrations in the United States, each with a variety of ballot styles, giving a total number of distinct ballot styles on the order of 100,000 nationwide. Any national solution to the problem of UOCAVA voting is immensely complicated by this!

We could immensely simplify the UOCAVA voting problem by a single simple constitutional amendment. Of course, such an amendment would be extraordinarily unlikely to pass. All we need to do is assign the voting rights of UOCAVA voters to a single election office, and expand the congressional representation of that office proportionally to the number of voters involved. This would probably involve a transfer of two or more congressmen. It might even be reasonable to have one or more congressional districts explicitly representing overseas civilians and others representing uniformed voters. The obvious jurisdiction for UOCAVA voters would be the District of Columbia, and the same constitutional amendment would have to extend full Congressional representation to the district for this to work.

Universal Identity Cards

The Internet voting system adopted in Estonia relies on the fact that every Estonian citizen is issued a national identity card. These are smart cards – that is, each contains a small computer chip and flash memory. Estonia uses these national ID cards as the basis for a national public key infrastructure that is used both in government and for commercial transactions. Every ATM and most home computers used in Estonia can connect to the national ID card. The Estonian Internet voting system uses this. Of course, the Estonian system relies on the fact that nobody would willingly loan their ID card to anyone else for even a moment. It is too valuable, too much depends on it.

The Dutch RIES voting system has its origins in an academic exercise, intended for use in student government elections, and it was originally developed based on the use of smart cards. Every university student has a student ID card, and these are smart cards at a growing number of campuses around the world, where they are used for functions ranging from charging textbooks and meals to unlocking doorways on campus. Extending the use of such ID cards to campus elections is natural.

In contrast, in the United States, outside of the military, we do not routinely track our citizens and we have a long tradition of resistance to any form of national ID card. For UOCAVA voters, the situation is somewhat more tractable. All UOCAVA voters have either a standard military ID card or a passport, but while electronically readable data has been embedded in passports and military ID cards for several years, UOCAVA voting systems have not generally been able to exploit this. Part of the problem is that there are two distinct formats, military and passport, and part of the problem is that there is a long tradition of putting passports in the custody of someone other than the holder. For example, in many countries, travelers are required to leave their passport at the desk for the duration of their stay.The Dutch RIES system was originally developed for

Are there any Secure Alternatives to the Post Office?

Postal voting for expatriate voters typically involve three postal transactions. The voter mails a request for a postal ballot to the appropriate election office. The election office mails the ballot to the voter, and the voter then mails back the voted ballot. Neither the Dutch nor the Geneva internet voting models eliminate the postal system.

In the Geneva system, the expatriate voter must inform the election office of his or her current address in order to receive a ballot. The election office routinely mails ballots to the current registered address of every voter who is entitled to vote, but for a highly mobile voter, the act of registration before an election is not significantly different from a U.S. voter mailing an request for an absentee ballot.

The net result for an expatriate voter in Geneva who opts to cast a postal ballot is the usual three-hop process. When Geneva introduced Internet voting, they did so with a very clever mechanism. The postal ballot mailed to the voter has, printed on it, a unique (and rather long) authorization code that may be typed into the voting web site in order to cast a ballot. This code is hidden under scratch-off paint using exactly the same technology used for printing scratch-game lottery tickets. The result is that the state does not know which ticket number was mailed to each voter, ensuring ballot secrecy.

If a voter opts to vote by mail (or in person at a polling place), they are advised not to scratch off the paint over the Internet voting authorization number. If they wish to vote by Internet, they scratch it off, type it into the web site, and vote on line. Any paper ballot received with the scratch-off paint scratched is set aside as a challenged ballot and is only counted if it has not been voted on-line. As a result, voters who are unsure whether their Internet vote was or was not recorded may mail in their paper ballots as insurance.

The Dutch RIES system is similar, except that voters were required to explicitly request either a postal ballot or an Internet ballot. Internet ballot authorization forms were mailed, and the mailed authorization included a similar (and rather long) ballot authorization code. Instead of using scratch-ticket technology, the Dutch used the printing technology commonly used for paychecks, where the printer prints legible text on the page inside the envelope after the envelope is sealed. Dutch ballots were not as thoroughly anonymised as those in Geneva because the RIES system, as deployed, allowed voters to request replacement ballots, and this required a mechanism to cancel a ballot that had been issued to a voter.

In sum, the net result, in both the Geneva and Dutch cases, is that the Internet voting mechanism eliminates just one of the three postal transactions required for expatriate voters. The use of the postal system to deliver the Internet voting authorization code is a central feature of the security of both the Dutch and Geneva systems.

Auditing

The designers of both the Dutch and Geneva systems designed them with significant auditing mechanisms, although they do it in very different ways. The Geneva auditing model is based on post-election surveying, while the Dutch model is based on universal verifiability and an end-to-end cryptographic scheme.

In Geneva, where each voter has the option of voting by mail, in person or by Internet, they do a routine post-election telephone survey of a random sample of the electorate. For each ballot received, they know whether it was voted by Internet, in person at a polling place, or by post. Furthermore, for ballots voted by Internet, they know if the same ballot was also received by post or delivered to a polling place. The question asked, by phone, is simple: Did you receive a ballot, did you vote, and if so, did you vote on-line, in person, or by post. If there is a statistically significant discrepancy between the answers received and the records of each ballot from the voting system, they know that there is a serious problem.

The RIES system issues, to each voter, a cryptographic receipt that may be used to check to see that the voter's ballot is indeed present in the on-line ballot box. After the polls close, anyone with sufficient expertise may check to see that the vote totals announced for the Internet component of the election matched the totals computed from the on-line ballot box. For those familiar with end-to-end verifiable

cryptographic voting protocols, this should be a familiar model. It should be noted, however, that RIES offers a degree of ballot secrecy comparable to postal ballots. It does not satisfy the strong receipt-free properties that most advocates of end-to-end cryptographic verification ask for.

The Rights of Election Observers

Dan Wallach at Rice University once quipped that the role of an election is to convince the losers that they really did lose. It is the losers who ask the hard questions, since once you tell the winners that they won, they are usually reluctant to ask any hard questions about the election. The result of this requirement is that elections need to be transparent. It must be possible for those observing on behalf of the eventual losers to see that the election was actually honest and open.

Election observation has always been difficult. With conventional polling places, each party must attempt to deploy observer to each polling place. The jobs of such observers are well established – observe that those who vote are actually on the voting rolls, that the number of ballots cast is the same as the number of voters, that no ballots are altered between casting and counting, and that voters are not subject to coercion.

When voting moves from the voting booth to the postal system, observation becomes more difficult. It is not possible to station observers in every post office, so we must rely on the postal inspectors to assure that no mail is diverted or opened in transit. It is certainly not possible to observe that individual voters are free of coercion, and in fact, it is well known that absentee ballot fraud, the buying and selling of absentee ballots, is a real problem. This is why many states have hesitated to move to a system of no-fault absentee voting.

When voting moves from paper into computers, observation becomes even more difficult. This was pointed out to me by Michel Chevallier, who said that the biggest mistake Geneva made when it first moved to Internet voting was the failure to provide election observers with adequate training. He suggested that observers at the computer center that is running an Internet election should have access to all of the same training and manuals that are available to the technicians running the election system. If the observers do not have access to the documentation needed to understand the activity that they are observing, then their observation is meaningless.

I believe that this observation applies to all election procedures. An observer at a polling place should have access to the pollworker manuals and training material so that they can tell if the pollworkers are acting correctly or are violating the procedures that they were trained to follow. This applies regardless of whether computers are involved.

I experienced this problem first hand observing the use of the RIES voting system in the Dutch parliamentary elections in 2006. I observed the opening and closing of the "Internet Polling Place" in Leiden, and I observed the activity in the Internet voting help center in The Hague during this election. Despite extensive access to supporting materials, including interviews with the developers and administrators of this system, I found that there were aspects of the system that were impossible to observe.

First, it is noteworthy that with Internet voting, key aspects of the voting system security are established at the very start of the election cycle, when the campaigns have barely begun to heat up and when observers are not yet ready to observe. In the case of the Dutch RIES system, the creation of the cryptographic codes and the printing of the envelopes that would later be mailed to every voter requesting an Internet ballot occurred before the international election observation mission I was on was organized. The higher the technology, the more this seems to be the case.

Second, most of what happened at the Internet polling place was, put simply, nothing. The Internet

election judges did nothing except fulfill a legal requirement that there be election judges at each polling place. All the real activity happened in servers that did whatever they were programmed to do. There was very little an observer could do to convince himself that the computers we saw had anything to do with the election process we were supposed to be observing. The end-to-end features of the Dutch system are valuable here, they offer some fairly strong assurance that they system did what it was advertised to do.

Third, in observing at the Internet voting help center, it was impossible to tell whether voter privacy was actually ensured. Voters could request replacement ballots by phone or e-mail. There was supposed to be a mechanism in place to prevent abuse of the ability to cancel ballots that had been issued, and to prevent the issue of unauthorized replacement ballots, but I cannot tell how to observe such a mechanism.

In sum, I feel that the developers of Internet voting systems need to put significantly more effort into thinking about how to observe elections carried out on their systems.