A Specification for Absolutely Accurate and Perfectly Private Election Voting Via The Internet

A paper submitted to EVT'08 on March 28, 2008

Marilyn Davis, Ph.D.
Deliberate.Com
marilyn@deliberate.com
*

Abstract

Absolute Accuracy is achieved by emulating a show-of-hands online. Once the online election is closed, everyone can see all the ballots and tally the results. Always, each voter can see her/his own ballot.

Perfect Privacy is achieved by giving an anonymous voter identification to each voter. It is the voter's responsibility to keep his/her real identity a secret, similar to voting by postal mail.

To prevent ballot-stuffing, the number of voters with anonymous online voter identifications (OPIK for Online Private Identity Key) must match the number of OPIKs in the online system.

The votes are kept in a distributed and redundantly checked network of computers, described in this paper.

Communication with the voter is via email, enabling confirmation and security.

The software and hardware are open, inviting everyone to inspect every aspect of the system.

Such a system must be voluntary, an addition to the current election systems. Any online voter wishing to go back to the traditional system must be allowed to rescind the online ballot and do so.

Because the ballots and the software are visible, this system is an *open-open election system* or OOES.

1 External Specification – The Voter's View

Voters will be asked to vote via the Internet, for these reasons:

1. For their convenience.
2. To be sure that their votes counts.

1.1 Registration

Each voter wishing to use the Internet voting system will request an electronic ballot in the same way that an absentee ballot is requested, with a signature mailed in, or by going personally to the local community registrar. See 2.1. Each voter wishing to vote using the Internet picks an anonymous Online Private Identity Key (OPIK) card from a box of cards. There is no record kept of which voter gets which OPIK card. See Figure 1.

*Thank you to many who have contributed ideas and discussion about voting online including Todd Davies, Charlie Davis, Mario Galvan, John J. Jacq, Evan Ravitz, and David Sederquist; and to Mary Bartholomew, Judi Kadish and Jim Stockford for editing.

Online Private Identity Key

Please Write Anything Immediately!

Voter ID: **XA325A**

See instructions on the other side.

Instructions for Voting

Go to:

http://vote.where.us.gov

Initial email address:

sunspot@vote.where.us.gov

Initial password: **Q1346bqZ**

Please write on the other side immediately!

Figure 1: **The OPIK Card.** Nobody, except the voter, knows which Private Identity Key belongs to that voter.

The OPIK card is a plastic card, similar to a credit card but with no magnetic strip or other high-tech devices. On it is printed an email address, an OPIK, a password, and a web address for further instructions. And, on the OPIK card, is a place to write something immediately. Only the voter can reproduce the writing so stolen or lost cards will be useless. The voter should not write her/his real name so that the voter cannot be identified from the card.. The voter will reproduce what is written, as well as her/his signature, in order to request a new OPIK card and a new online ballot; or to vote in the traditional manner.

A card will expire in a year or a few years, requiring re-registration. Each voter can decide when his/her OPIK card should expire, weighing the benefit and danger for themselves.

With the data printed on the OPIK card, the voter logs onto URL address given to access the email address given and changes the password, and if desired, the email address associated with the OPIK. These changes are protected with a confirmation process. See page 4.

The OPIK is a permanent characteristic of the OPIK card and is necessary to prevent ballot-box stuffing. See Appendix C.1.2.1.

1.2 Voting

Critical to the security and convenience of this *open-open election system)* OOES is the fact that it is email-based (See Appendix B), and that voters have time to exchange many emails with the OOES.

The OOES opens for voting some weeks, maybe three, before election day and voters can vote online until it closes, maybe one week before election.

At any time, up to and including election day, the voter can use her/his OPIK card to cancel her/his online ballot, and choose to vote in the traditional manner instead.

To vote in an election:

1. A voter begins voting by emailing a filled-in ballot to the vote system using his/her registered email address in the `From:` header. To facilitate this step, the voter can:
   - use any one of many official web sites to click choices.
   - use a computer program to help generate the filled-in ballot.
   - send a request to the OOES and receive detailed instructions for generating and sending the email ballot manually.
2. The OOES emails a *confirmation request* back to the voter which contains a copy of the entire ballot, as it was received, and an image, i.e., a *Captcha*. See Appendix B.4

3. The confirmation requests that the voter check the ballot carefully, then click the reply-to button, and type in the Captcha, to send a *confirmation reply*.

4. After receiving a correct confirmation reply, the OOES emails a *vote receipt* to the voter. The receipt contains the recorded online ballot.

5. The OOES closes and, one or a few days later, the OOES no longer accepts confirmation replies. Also, at that time, the OOES sends each online voter a *final receipt*, again displaying the voter's recorded online ballot.

At any time while the election is open, the voter can send an email request to review the ballot.

At any time before the election is over, the voter can cancel the online ballot by taking her/his OPIK card to the registrar, or to the polling place, and show that s/he can match the handwriting on the OPIK, and sign his/her real name.

At any time while the OOES is open to voting, the voter can take the OPIK card to their registrar to cancel the online ballot, and be issued a new one if time permits.

Once the election is over, each and every voter can see all the electronic ballots and check all the statistics; and see and check her/his own ballot.

1.3 Voter-Maintained Privacy

In this OOES, voters are responsible for maintaining the privacy of their own ballots. A list of voters who have online ballots and a list of OPIKs is public; but no information about which online voter has which OPIK and associated ballot is kept. Only the voter knows which OPIK is hers or his. See Figure 2.

One week before election day, the OPIK cards that were not given to voters are used to delete the unassigned online ballots. The registrar must ensure that the number of remaining active online ballots and the number of online voters match exactly.

The voter, when first receiving a OPIK card is cautioned to:

- Immediately write on the OPIK card so that only the proper voter can bring the OPIK card to the registrar to cancel or re-issue the associated online ballot.

- As soon as possible, go online to change the password so that the ballot cannot be stolen, even if the card is stolen.

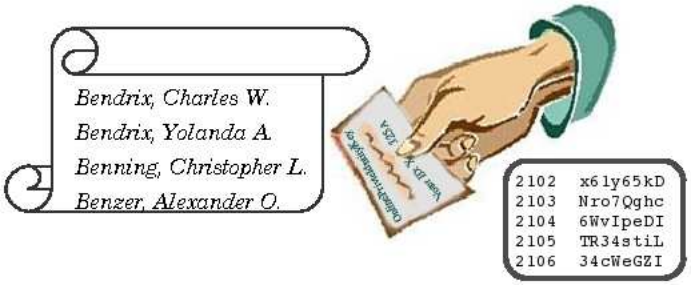

Figure 2: **Voter-Maintained Privacy.** The OOES maintains public ballots, each with an associated OPIK, and a list of online voters, without the associated OPIK. Only the voter knows which ballot and associated OPIK is hers/his.

Once the voter has written on the OPIK card and changed the password:

- Only the rightful owner can access the online ballot because the password has been changed.

- Only the rightful owner can reproduce the writing to cancel the online ballot and/or obtain a new online ballot.

Therefore, once the OPIK is written on, and the password changed, the online ballot is secure against theft from outside the system, even if the OPIK card is lost or stolen.

For convenience, a voter can change the email address associated with the OPIK card and associated online ballot. The process is:

1. The voter sends an email request to the OOES for the address change, using the old address.
2. The OOES sends two confirmation requests: one to the new address and one to the old address.
3. The voter must return both confirmation messages.

The OOES must remember the original and any subsequent email addresses associated with each online ballot. This is important because, if a voter wishes to cancel his/her current online ballot, the OOES must follow the chain of email addresses to delete the correct online ballot.

Summary of the Online Voting Process

An online voter follows these steps:

- Before the election:
  - Write on the OPIK card, not writing her/his real name.
  - Go online and change the password, and optionally, the voting email address.
- From the time that the online poll is closed to shortly before election day:
  - Send an email ballot to the OOES.
  - Receive and check the confirmation request, which includes a Captcha.
  - Send the confirmation request back to the OOES, providing an answer to the Captcha.
  - Receive and check the vote-receipt.
- During the period after the online poll is closed and the election is over:
  - Receive and check the final receipt.
- Optionally, at any time:
  - Send a request to view the online ballot.
  - Receive and check the online ballot.
- In the event of a discrepancy, or a change of mind:
  - Before the online poll is closed:
    - Bring the OPIK card to the Registrar of Voters and cancel the online ballot; and optionally if there is time, obtain a new one.
  - Otherwise:
    - Bring the OPIK card to the polling place to cancel the online ballot and vote in the traditional manner.

2 Internal Specification – Implementing the Vote System

2.1 A Community's Computer and Administrator/Registrar

Each geographical area of (perhaps) 2000 voters will have at least one inexpensive computer running the GNU-System (often called Linux) connected to the Internet. All software will be open source.

The citizens who reside in a particular geographical area for the purpose of this specification, are that area's *community*; the computer and administrator/registrar for the area are the area's *community* computer and administrator. The community administrator is also the registrar for the community's online activities.

A community's administrator will be a local person, trained, certified, and ideally, elected by and known to the community. When citizens choose their own administrator, they assume ownership and take responsibility for their system. This is always important in democracy, but particularly important for an OOES because citizen participation is critical to the stability and accuracy of the system.

The system will be automated to the point that the administrator's technical role is very small. The administrator's responsibilities may be limited to providing face-to-face registration services, maintaining the hardware and connection, assisting community members who wish to inspect the physical computer and Internet connection, and providing technical help for the voters in the community who are participating online.

The community computer will be maintained in a library or school and be in place and functional all the time. Besides providing elections, the system can be used to facilitating other community-centered activities.

The community computer will be open to physical inspection by members of the community, as well as voters everywhere and trained inspectors. All programs and data will be available for read-only access via the Internet, except, while an election is in progress, only the voter who owns a particular ballot will be able to see that ballot. This small amount of temporary secrecy is necessary so that it is not possible to deduce the vote tally until the election is over.

2.2 A Community's Ring of Computers

The OOES is a system of all the community computers communicating with each other through the Internet.

The linchpin of the system is the fact that each community computer can, in addition to acting as the main point of responsibility for its own community's votes, simultaneously provide verification services, backup and data-checking for other communities [1]. Each community computer provides and reinforces security for other community's computer by forming a complex dynamic network with constant redundant checking. This is how a public show-of-hands is provided by the OOES.

The point of the network design presented below is to ensure that at least three administrators must collaborate to cause even minimal and temporary damage to even a small part of the system. The three elected administrators do not know each other before they collaborate in the OOES; and, two of the computers in the ring will be swapped for other computers and administrators at random intervals.

This random swapping will take some time to complete, while the domain's new configuration travels around the Internet. While the swap is taking place, there will be an extra computer in the ring so that the the ring remains responsive to voting requests.

To accomplish this level of security, the community computer and administrator are the main point of responsibility for a community's ballots; and at least two other community computers (and administrators) randomly chosen from all the community computers in the OOES, participate in the community's *primary ring* of computers. The ring of computers for the Red Community, an example community, is pictured in Figure 3.

All three computers in the ring share the responsibility of receiving ballots for the Red Community, generating and receiving confirmation messages, and tallying results.

This is possible because the Internet email system can be configured by a domain owner so that, when an email message is addressed to that domain, the system sends the message to one of many designated computers. (See Appendix B.1. In the OOES described here, the mail system will randomly pick one of the three computers for each email message. This random picking happens on-the-fly, i.e., when the email is routed; no one can predict which computer will actually receive the email message.[2] See Figure 3.

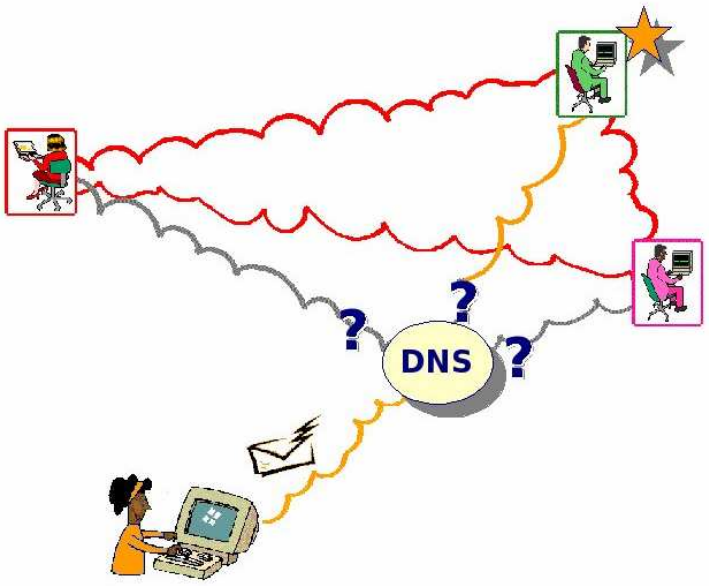

Figure 3: **An emailed ballot is destined for one computer; exactly which one is chosen randomly and on-the-fly by the Domain Name Server.** An emailed ballot arrives at one of the computers in the Red Community's primary ring of computers. The ballot is acknowledged by all the computers in the ring before the voter receives a confirmation message or receipt.

2.3 Data Collection Procedures

When a ballot is received by one computer in the Red Community's ring, all three computers communicate, via a specialized protocol through a port with a higher priority than email, to communicate and mutually acknowledge the incoming ballot, as well as all the email headers that the message contains. All three participate in the generation of a confirmation request that bears a *message authentication code*, or MAC, from each of the three. A MAC is a standard encryption technique for eliminating the possibility of falsifying messages from system. [1]

Finally a confirmation request is emailed from one of the two computers in the ring that did not receive the original ballot, also randomly chosen. The incoming ballot message is stored on all three computers along with a record of which computer originally received it, which computer was chosen to send the confirmation request.

The ballot is not entered into the election data until the OOES receives the confirmation from the voter.

When the confirmation reply is received from the voter, again all three computers participate in the generation of the final receipt, again carrying all the email headers of the incoming confirmation reply, the original email ballot, its headers and MACs, and bearing new non-repudiation MACs from all three computers. The receipt is emailed to the voter by one of the two computers that did not send the confirmation request.

All three computers in the primary ring are required to participate in the direct communication with each voter:

- One computer receives the original ballot; a different computer in the ring is required to send the confirmation request.

- One of the two computers that did *not* send the confirmation request is required to send the receipt.

2.3.1 A Malfunctioning Computer

When, during the formation of the confirmation message or receipt, it is detected that one of the three computers in the ring is malfunctioning or missing from the network, the primary ring is immediately and automatically expanded so that at least three functioning computers have stored all the community's vote data and statistics, and all three must acknowledge receipt of the message. The scheme listed on page 6is still followed for choosing which computer sends the confirmation message or receipt.

Note that, while a ring is in this semi-repaired condition, although three computers are engaged in each communication, and any of the three can send email; the DNS only has two computers to choose from when routing OOES-bound email.

If a malfunctioning computer is out of service for more than a day, the OOES updates the DNS system so that, once again, three computers can receive email for the community and the ring is completely repaired.

If the simultaneous failure of all three computers in a ring is deemed likely, the ring can be expanded to include more computers and administrators.

The cost of expanding the ring will be an increase in response time for the voters and more memory usage.

Section 2.4 and Section 2.6 specify two more safeguards to build into the network.

2.4 A Secondary Ring

Another layer of security can be implemented for the Red Community's data where three computers on the network, not in the Red Community's ring, carry a real-time copy of the Red Community's data, transmitted through the high-priority port mentioned on page 6. These additional computers will be backup-only, meaning that they will not, under ordinary circumstances, receive and send email for the Red Community, but will be ready to do so, if the need arises.

These additional computers will be listed in the DNS as *second-priority* recipients for email for the Red Community. Under ordinary circumstances, the DNS will choose one of the first-priority computers, which are the Red Community's *primary ring*, to receive mail for the Red Community OOES. If all three of the computers in the Red Community's primary ring fail simultaneously, the DNS immediately and automatically routes email to one of the second-priority computers, also randomly chosen.

The arrival of a Red Community email message to one of the computers in the secondary ring will trigger the secondary ring to query the primary ring through the high-priority port to determine if the incoming email should be deferred (Appendix B.2) because the primary ring is busy, or if the secondary ring should become the primary ring for the Red Community. The new primary ring will find three more computers in the network to form a new secondary ring for the Red Community, and designate, in the DNS, these computers as third-priority destinations for the Red Community's email, if yet another layer of security is deemed desirable.

Whenever the Red Community's computer is functional, it must be put back into the primary ring.

2.5 The Network

In the simplest and least redundant, and therefore least secure, configuration (i.e., three computers in a community's primary ring and no secondary ring) the Red Community's computer, while serving as the main point of responsibility for the Red Community's vote data, must also serve on the ring of computers for two other communities, the Blue and Purple, and is therefore in high-priority communication with four more computers. See Figure 4.

In this configuration, each computer maintains six active relationships with other computers. To minimize vulnerability, the six relationships must be with *different* computers, so that when one computer fails, there are three unrelated small holes in the network to fill. If instead, the Red, Green and Pink computers were to be the primary rings for each other, then, if all three computers were to fail simultaneously, the primary ring vote data for all three communities would be compromised. If they fail simultaneously but have only one relationship with each other, that is to form the Red Community's primary ring, only the Red Community's vote data would be affected. However, the secondary ring for the Red Community would be ready to step in to become the primary ring.

The smallest network where each computer has six relationships with six other computers, is a network of seven computers, pictured in Figure 5.

The numbers and diagrams given here are for maintaining three computers in a community's primary ring, and no secondary ring.

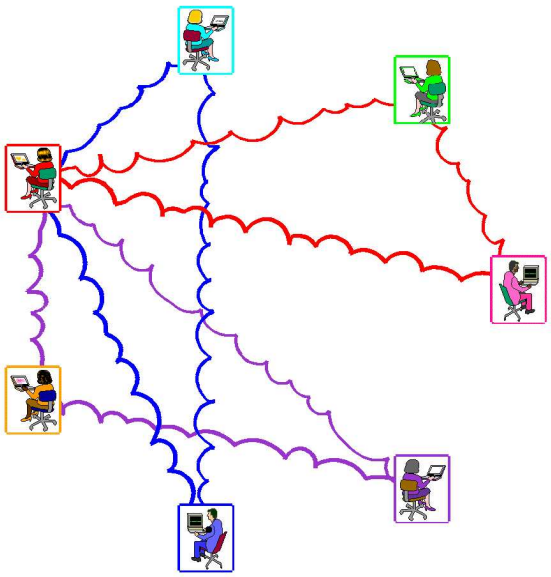

Figure 4: **The Red computer's relationships.** The Green and Pink community computers participate in the Red Community's ring; the Red computer works with the Turquoise Community's computer to form a ring for the Blue community; and the Red Community's computer works with the Gold Community's computer to form the ring for the Purple community.

The scheme can be expanded to maintain many computers in the primary ring, and many more in layers of secondary rings, if three are considered to be insufficient.

2.6 Backup Procedures

Each computer must keep a complete log of everything that it does to ensure every opportunity for recalls and redundant checking forever.

All computers must keep at least two off-site backup copies of all data and logs on a *backup-host* computer: one backup copy of all the data is refreshed each hour, the other backup copy is refreshed twice a day. Two backup-host/backup-client relationships exist for each computer in the network; each computer is the backup-client to a backup-host; each computer is the backup-host to another computer, its backup-client.

Note that a backup-host keeps backup data for one computer, but that that computer is in the primary ring for three communities. So each backup-host is, in effect, providing backup service for three communities.

The backup-host is randomly chosen from all the computers in the OOES that are not already involved with any of the data in any of the three primary rings serviced by the backup-client.

When a computer breaks, for example the Red Community's computer, procedures must be in place so that its responsibilities are assumed by four other computers in the OOES:

1. One computer in the OOES takes the role of the Red Community's computer for the Red Community, in addition to being the community computer for its own community.

2. The Red Community's computer, now broken, was in the primary ring for at least two other communities: the Blue Community and the Purple Community. Two different computers in the OOES

automatically take responsibility for the broken computer's duties in regards to each of the other community's data processing.

3. The Red Community's computer was the backup-host computer for at least one other computer in the OOES. A computer in the OOES must automatically serve as that backup-host.

Procedures must be in place in the software so that:

1. The two remaining computers in the broken primary ring find four computers in the OOES to replace the broken computer. The four computers are chosen randomly, except that care is taken to ensure that no computer serves more than one role in any community's data and so that the work load is distributed approximately equally.

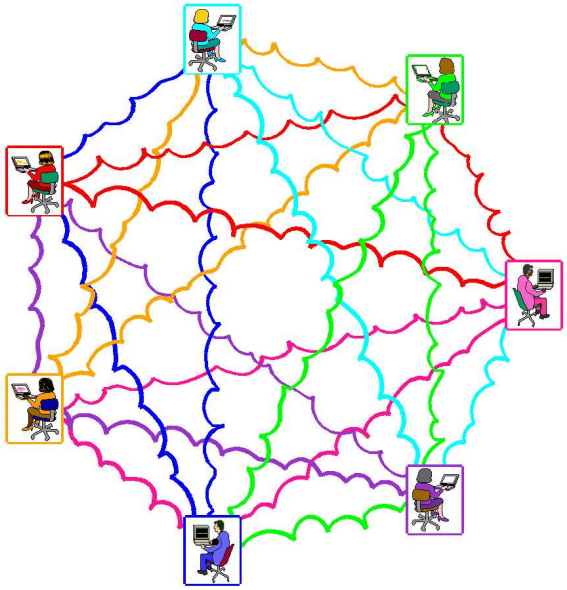

Figure 5: **The minimal network.** A minimum of seven computers is required in the network to keep three independent dynamic copies of the vote data for each community served by the network. More computers are added to configure a secondary ring for each community, and to make back-up copies of the vote data for each community.

2. Each computer that assumes a role in a particular community's primary ring collects the data that is pertinent to that community from the backup-host and the two remaining computers in the ring and checks that the data from all three sources are consistent.

3. The computer that becomes a backup-host in place of the broken computer must collect fresh data from the client computer and check that the data are consistent with all three of the client computer's primary rings.

2.7 An Arbitrary Amount of Security for each Ballot

In summary, when all the redundancy and backup procedures described above are in place, each voter's ballot is recorded on 12 computers in the OOES:

1 On the voter's community's computer.

2 On the other two computers in the voter's community's primary ring.

3 On the three computers in the voter's community's secondary ring.

6 On the six backup-hosts for each of the six computers listed above.

12 Total copies of each ballot scattered through the OOES.

The design can be expanded in several directions to provide even more redundancy and checking:

- The primary ring can include an arbitrary number of computers.

- Besides a secondary ring, an arbitrary number of lower-priority rings can be established.
- Instead of one backup-host per computer, there can be an arbitrary number.

Additionally, except for a community's computer, all the other computers involved in maintaining data for a community can be randomly swapped so that different computers and administrators collaborate with the community computer on different days.

In summary, the amount of security available for vote data is virtually unlimited.

3 Conclusion

Internet voting in an open vote, open source network offers unprecedented opportunity for election security.

While such a system offers rigorous safeguards for the ballots and the accuracy of an election, the integrity of the system depends on the vigilance of the voters themselves.

A The Trade Off

The Open-Open Election System outlined here exposes a trade off inherent in any voting system: vulnerability to *retail fraud* vs. vulnerability to *wholesale fraud*.

In our traditional systems, the ballots are completely anonymous and voters have no idea what really happens to their ballots, or if the tally is correct. Voters must trust the system. In the traditional systems, there is little opportunity for vote-selling or coercion. Note that this safeguard is completely gone when voting by postal mail.

The foundation of this OOES, is that, because of the openness, voters can prove to themselves that their ballots are accurately counted, and that the final result is an accurate tally of the all the ballots.

In an OOES, voters are responsible for their ballots and for watching the election; there is nothing about the system that demands trust.

However, in an OOES, if, as a voter, I can prove to myself that my vote was counted accurately, then I can prove it to someone else.

Therefore, an OOES such as this one has no built-in mechanism for preventing *vote-selling* and *coercion*. In *vote-selling*, because I can prove how I voted, I can sell my vote. In *coercion*, I can succumb to threats of violence, job-loss, love-loss, etc., from a blackmailer because I can prove that I voted according to the dictates of the blackmailer.

A.1 Ineffective *Retail* Fraud vs. Undetectable *Wholesale* Fraud

In the election business, vote-selling and coercion are categorized as *retail* fraud, ballots must be bought or coerced one ballot at a time. Ballot-box stuffing, switching of ballots, losing ballots and deliberate miscounts, which are perpetrated from within the traditional election systems, are *wholesale* fraud and can affect thousands, or hundreds of thousands, of ballots in one operation, and may never be detected.

Choosing to prevent vote-selling and coercion for some (non-mailed) ballots by exposing the election system to wholesale fraud is a poor choice. But before the computer network, it was the only practical choice.

This OOES chooses to eliminate *wholesale* fraud and to accept and manage any *retail* fraud.

The point here is that retail fraud is much less likely to happen, less likely to be effective, and less likely to go undetected than are the wholesale fraudulent techniques possible in current election systems.

Other points about the wholesale/retail fraud trade off:

- Prevention/detection of wholesale fraud that happens inside any election system is the responsibility of that election system. However, only an OOES allows the voters to expose, detect, and therefore prevent, inside fraud.
- Because retail fraud happens outside the election system, detection and prevention belongs outside the election system, i.e., with regular law enforcement.
- Vote-buying and coercion, that is to say, retail fraud, is not practical:
  - Retail fraud requires soliciting cooperation from voters, one voter at a time. The probability of being caught increases with each voter approached.
  - If a reward is offered for information that leads to the apprehension of a vote-buyer, the cost of buying each vote must be much higher than the reward. Ruining an election by buying votes is prohibitively expensive.
- Vote-coercion by familiars is a more likely scenario. It is no more likely to happen in this OOES than it is when voting by postal mail, which is accepted in many states.

B Voting by Email

Email is the perfect medium for voting, superior to the WWW for several reasons:

1. Built into the Internet is an important device for maintaining the sturdiness and flexibility of the email system, and therefore, the OOES: the *Domain Name Server* or DNS, a distributed database that is used to route email and URL requests to the appropriate computer.[2]

   Each computer on the Internet has an *Internet Protocol* address, or *IP address*.

   The owner of a domain name (like xxx.org, yyy.com, etc.) configures the DNS to deliver its incoming email and requests for web pages. The domain name owner specifies one IP address for web requests, but configuration is more complicated for email:

   - When a request is made to send an email message to an address at a particular domain, the DNS routes the email message to one of many computers:
     - The DNS will randomly choose one of the IP addresses designated as first-priority by the owner of the domain. This will be one of the computers in the primary ring.
     - If all the first-priority computers are non-functional, the DNS will randomly choose one of the IP addresses designated as second-priority by the owner of the domain. This will be one of the computers in the secondary ring.
     - If all the first-priority and second-priority computers are non-functional, the DNS will randomly choose one of the IP addresses designated as third-priority, etc. A tertiary ring is not specified here, but could be.
2. If all the computers that have been designated to receive email for an address are not answering, either because they are busy, or because they are broken, the email will be *deferred*. This means it will be stored on the sending machine and delivery will automatically be attempted later, and again later, over and over, for up to several days. Humans are not inconvenienced. This characteristic of email, renders a DOS, or *denial of service* attack, i.e., flooding the system, ineffective.

3. Email can be verified to have a truthful address in the `From:` header by using a confirmation procedure: after receiving an email ballot, the vote-server sends back a confirmation request. Although the original email can have a forged `From:` address, the confirmation request can only go to, and be confirmed by, the correct email address.

4. Although email is susceptible to virus, and in particular a virus that could intercept and confirm a confirmation request, a virus, or any program, is not capable of reading distorted characters that are shown as an image, rather than text. A system that uses this fact to verify that a real person, and not another computer program, is responding is called a *Challenge/Response* system. A machine cannot provide a confirmation reply. [3]

5. Last, but most important, with email, the voter and the OOES can be in constant contact, making redundant checks as necessary at almost no cost.

Although email is the best conduit for voting online, email can be cumbersome to use compared to a WWW interface. However, a web page or any computer program can prompt the voter for votes and generate and send the initial email ballot to the email-based vote system.

C Threat Analysis

The motivation for the OOES outlined here is the following list of the types of threats that a voting system faces:

C.1 The vote data can be attacked:

C.1.1 There can be hardware failure.

The simplest version of the OOES specified here (see Section2.2) demands that all three computers in a ring be compromised simultaneously in order to damage or lose the vote-data for a particular community. If one or two of the three computers are compromised, the broken computers are immediately and automatically replaced by other computers in the network, ensuring that there are always at least three live copies of the vote data for the community, and that two of the copies are on random computers.

There is also provision for placing more computers in the ring, for implementing a secondary ring of computers, and/or maintaining scattered backup copies of data and logs, if all this is considered necessary.

Finally, all transactions are logged so that, if disaster strikes, the vote-data can be recovered and any voters whose ballots may have been affected can be notified and asked to re-confirm their ballots.

C.1.2 An administrator within the system can attack the vote data.

Breeching voter privacy is not an issue because the privacy of voters is protected by their anonymity, which the voters themselves maintain, or not, as they choose.

An administrator must work alone to subvert the system as he/she will not know the other administrators in the rings with which he/she participates, and these other administrators can be occasionally exchanged for other administrators. See page 5.

1.2.1 Stuff the ballot box with bogus ballots.

The list of active online voters' names for a community is public; also the list of active OPIKs is public. The correspondence between names and OPIKs will not be known.

Everyone can count that there are the right number of voting identities, and that exactly those online voting identities, and only those identities are represented in the data. See Figure 2.

1.2.2 **Falsify data for a legitimate ballot.**

In order to successfully falsify a ballot for a voter, the administrator must identify a ballot that has not been used, and that will not be used by the intended voter. Already, this is very unlikely to be successful, even for falsifying one ballot.

Still, if an unscrupulous administrator tries this, then he must communicate a false ballot to the other two computers in the ring, and suppress both the request for confirmation and the final vote receipt. Because these two messages are sent from different computers, and the unscrupulous administrator can only have control of one, it is impossible to suppress both of them.

1.2.3 **Publicly release the ballots before appropriate.**

Releasing all the ballots before it is appropriate is undesirable because this would allow an early tally of the ballots that are in the system.

The software is designed so that, before release of the ballots, a ballot is only emailed to its associated address. Standard encryption techniques and law enforcement are used to prevent an administrator from releasing ballots early.

1.2.4 **The statistics can be falsified.**

Falsifying the statistics, i.e., the vote tally, is impossible because all the ballots are available to everyone, and everyone can calculate the winners themselves. This is the online emulation of a show-of-hands.

1.2.5 **Wreak havoc.**

A system administrator could attempt to wreak havoc by sending garbage data to the other computers on the network. This would quickly be interpreted as a broken computer, the computer would immediately be isolated from the network and replaced. The vote data would not be affected.

A system administrator could wreak havoc by sending false receipts and confirmation requests. This would be quickly detected and the computer would be dropped from the network and replaced. The vote data would not be affected.

C.1.3 **The vote data can be attacked from outside the vote system.**

1.3.1 **Email communication can be attacked.**

The only way for data to enter the system once the election is open for voting is via email. Every ballot confirmation is verified to originate from the voter's address by a back-and-forth email communication via the confirmation process. Until it is properly verified, a ballot has no effect on the vote data. See page 2.

Therefore, the only threats identified are:

1.3.1.1 **A denial of service attack.**

This threat is discussed in Appendix B.2.

1.3.1.2 **A specialized email virus.**

This is discussed in Appendix B. 4.

1.3.2 **Communication between computers in the OOES can be attacked.**

The communication between computers in a the network can be protected by standard encryption techniques. Authentication is important. Each computer must know which other computer sent each message.

Because the network is closed to non-email communication from computers outside a known set of computers, and because the administrators of the computers can be in con-

tact via telephone and registered postal mail to share keys, the problem can be solved with known techniques. See Appendix D.

Even if the network was compromised, an outside attacker would face the same obstacles that an unscrupulous administrator does. See Appendix C.1.2.

1.3.3 **The DNS can be attacked.**

A successful DNS attack would threaten the Internet so the DNS is already well-protected. This part of the specification needs to be developed by a DNS expert.

C.2 **A voter can falsely claim that his ballot is recorded incorrectly in the vote data.**

In order to claim an error has occurred, the voter must produce his OPIK card, which points to his online ballot, and show a confirmation request and vote receipt. Each confirmation request and vote receipt will carry a *non-repudiation Message Authentication Code*, or MAC, a standard encryption technique, which proves, or disproves, with absolute certainty, the validity of the confirmation request or vote receipt.

A voter who has not voted will have no receipt or confirmation message and will have no way to prove that he didn't vote.

Similarly, a voter can claim that the data in his online ballot was changed since he voted. For these reasons, it is important that the OOES be closed to voting for a week before election day. During this week, each voter is asked to check her/his online ballots and rescind her/his online ballot and vote in person if she/he sees a discrepancy, or if she/he simply wants to vote traditionally.

D Encryption Techniques

Because the OOES is an open system, encryption will not be used to provide privacy. Each voter protects his/her own privacy, as described in Section 1.3.

Encryption techniques are needed to:

- Ensure that each computer in the OOES knows with certainty with which other computer it is communicating.
- Detect and expose any attempts to falsify communication from the OOES.
- Temporarily hide the individual ballots from the system administrator so that they cannot be released to the public before the election is over.

Mechanisms for providing these security facilities exist and are well known. However, this part of the specification needs to be developed by a security expert.

References

[1] Marilyn Davis. *Protecting a Vote System From Attack From Within* `http://www.deliberate.com/wote01/wotetext.html`, Paper presented at *WOTE'01*, Tamales Bay, CA., 2001.

[2] Phillip Hazel. *Exim - The Exim SMTP Mail Server*. UIT Cambridge, UK. 2003.

[3] Wikipedia. *Captcha*, `http://en.wikipedia.org/wiki/Captcha`