600.443 - Security And Privacy in Computing
Johns Hopkins University

6 March, 2003

E-VOTING DESIGN DOCUMENT

prepared by: Charles Wright
Dan Kalowsky
David Friedman
John Daniel

TABLE OF CONTENTS

Registration

Voter registration is the largest and most difficult of the problems facing the electronic voting system. Although creating a database is relatively simple maintaining it can be difficult because people relocate without notifying election officials.

Registration Procedure

Let us first discuss how a person registers. A citizen of the state can register through the mail or at a variety of government funded public places (the DMV, public library, the post office, the unemployment office, etc.). They must meet four requirements in order to register:

1) Be a citizen of the United States
2) Be a legal resident of Washington State, your county, and your precinct for at least 30 days immediately preceding the election to vote in
3) Be at least 18 years old on the day of the election
4) Not be convicted of a infamous crime, unless restored to civil rights

A person must register at least thirty days in advance of the election.

The voter registration card contains the voter's registered address, precinct, and legal name. This card allows a voter into a polling station to place a vote. The card can utilize many of the anti-counterfeiting technologies also seen on money and checks (e.g. color changing ink, watermarks, etc). The state government distributes the cards. Those voters who register but do not receive cards should contact their local election official.

Database Data

The database contains the minimal necessary amount of information about each voter:

1) Voter Name
2) Voter Address
3) Date of Registration
4) Date of Birth
5) District

The state of Washington does not require a voter to declare a party affiliation at the time of registration (http://www.fec.gov/votregis/primaryvoting.htm).

It is unlikely that there will be two different people for which all five parameters are the same

Database Maintenance

We have yet to figure out a means of allowing a voter to automatically update their registration information. Until such a means can be conceived, we propose that each voter send in an updated registration request with their previous and new information. Looking at the registration results for Washington State during the 1995-1996 election (see http://www.fec.gov/votregis/nvra2.htm) this does not seem to an unreasonable request. With 39.64% registering via the DMV, and another 37.39% registering through the mail, it seems that providing a DMV agent a means for directly altering the registration database could potentially increase accuracy as well.

One problem with providing each DMV station access to the database is the potential for the database to not respond (due to network lag or disruption possibly). It's not very likely that you can ask a potential voter to return another day when the database is working. One proposed solution is to provide each DMV with a local copy of the database through a series of replications that occur after the close of business. Database replication is a well studied and known technology, as such it can be implemented with high level of accuracy and reliability.

The replication can utilize an online connection to synchronize the databases. Since it is not essential that the database be synchronized nightly, the effects of a denial of service attack would be minimal. At worst, the fallback and use of a dedicated line to cause the synchronization can be utilized.

Ballot

Each district has their own ballot corresponding to what offices are up for election in that state. However, under our system a voter may vote in any poll site anywhere in the state. Therefore, we need some mechanism such that a voter on entering a poll site receives the proper ballot.

Ballot Creation and Distribution

Under this system, each voting district will have to submit a certified ballot to a central state government based collection agency before a given timeframe. The state agency will then compile each ballot into a database, and distribute this information via a non-rewritable media to districts along with the registered voter list before an election. Each media distributed will also be digitally signed allowing confirmation of its authenticity.

The use of an electronic submission method is suggested for speed. In a situation where a ballot has not been received by the deadline, a state representative will contact the district in question. If the delay is due to a technical reason, a backup method for a non-electronic method is provided using a non-rewritable media. In the case where a ballot is delayed due to political conflict, the state may submit the issue to the courts for a ruling on an expedited track.

Ballot Format And Certification

To certify a ballot, a quorum of local elected council members needs to electronically sign and verify the ballot and options. The contents of this ballot can be an XML based file, and a hash of the file contents (see Appendix A). The choice of an XML file allows for an independent method of displaying data, but contains the bare minimum data for a ballot. This allows a voting device to be configured for use with handicapped voters, and possibly those who have difficulty in seeing without impeding the data. This change also opens up a possibility of vendor rendering techniques to differ. With this difference there is a possibility of a displayed ballot to look different from machine to machine. It is possible to correct ballot display with a tighter definition on the DTD and XML format, but we will discuss this later on.

We will use SHA1 as our secure hash since it is a federal standard (http://csrc.nist.gov/CryptoToolkit/tkhash.html).

Voting

Voting Day Preparations

On voting day, each polling station should have a copy of the registered voter database and the ballot database. These will be loaded onto a local server, and connected via a private network to a workstation for each of the poll station volunteers to use. Each volunteer will sign in allowing them to interface with the database. An electronic audit will be kept of how the poll workers use the database.

Each workstation will be provided with a keyboard, a signature pad, a monitor, a magnetic card reader/writer, and a push button booth activation device.

Sample Voter Arrival

In the following we describe the steps a voter takes in the voting process:

Step 1: Identify the Voter

When a voter arrives at a poll station, they are asked to relinquish their voter registration card. Parts of the information on the card will now be entered into the workstation allowing a search of the registered user database, and present the results to the volunteer. If multiple results are returned, the search can be further tuned by adding in further data from the registration card.

Step 2: Issue the Ballot Card

Once a voter has been identified, they are to add their signature to an electronic recording pad. The signature sample is now stored along with name of the poll volunteer and the time of the transaction. During this time, the poll volunteer places a magnetic media card into the writer, and places data identifying the proper ballot for the voter. This ballot card need not be encrypted. It can be presented in plaintext identifying the voter

district. In unencrypted form, a poll volunteer would be able to visually (via a card reader) check and confirm that the data has been written correctly. The use of this ballot card will be similar to that of an ATM card, providing a voter with access to a voting machine.

Step 3: Open the Voting Machine

All the voting machines work in the following way: they accept a single ballot card and then shut down waiting for the poll worker to open them. The purpose of this measure is to prevent voters from obtaining multiple cards and using them all in a single voting session.

For example, each poll site worker station could be equipped with a small panel with a series of buttons on it. The buttons on this device correspond to the voting booths in the poll site. Every button has an internal multi-colored LED with a color corresponding to the current state of the voting booth. The voting booth is enabled by pressing a lit button on the worker's panel, and is automatically disabled by the booth itself when it properly records a ballot.

Step 4: Vote

After voters have entered the booth, they will be presented with a monitor, a card input reader, and large voting buttons on the front of the device. These buttons could be similar to those on a typical soda vending machine.

After the voters have entered the ballot card into the voting machine it will present them with the ballot and ask them to confirm or deny that this is the correct ballot for their district. If they select yes the individual elections will be shown to the user with names and relevant information, as well as a number denoting which of the large buttons to press.

In particular we do not recommend using photos in the interface because they may influence a voter’s opinion in some way. Also photos take up unnecessary levels of screen space.

After the vote has been confirmed, the process repeats for all elections on the ballot.

Step 5: Print out a paper copy

To the side of the monitor displaying voting options is a large window protected by a clear plastic cover. Upon confirmation of the last vote, a printer inside the machine produces a paper copy of the ballot results in a format that is both human and machine-readable.

This paper ballot will pause in front of the plastic window, and the monitor will once again ask the voter for confirmation. The user will then inspect the results of their ballot, and press a button to accept or reject. A rejected ballot will be fed into a discard pile which is visibly destroyed in front of the viewer allowing the voting process to be restarted. The system however will lock up and call a poll attendant if the voter uses up more than a certain number of ballots.

If the ballot is confirmed, it is fed directly into a locked bin attached to the rear of the machine for the purpose of keeping a paper trail. At this point, the voting machine sends the results of the ballot via shielded cables to the tallying machines located at the polling station and receives confirmation from the tallying machine that the vote was received and recorded correctly. At this point the voter may leave the booth.

Cleanup

The magnetic card inserted by the voter at the beginning of the session is cleared of its memory, and filed into another bin at the rear of the machine for collection and reuse by the volunteers.

Other Voting Details

Paper Audit Trail

Finally, the system of collecting an auditable paper trail must be described in more detail. As was described previously, the ballot shown to the voter is filed into a locked bin at the rear of the voting machine. Actually there are two bins that are collecting votes at the rear of the machine. The larger bin collects votes that are cast by voters in their home district. A second, slightly smaller bin is used to collect all ballots cast by voters from outside the district in which they are voting for. In this way, it is much easier to distribute paper copies of foreign ballots to their appropriate locations without having to disturb and risk contamination of ballots from the home district. These may remain in the locked box until it becomes necessary to review the paper trail for recount purposes.

Lost Voter Registration Card

When a potential voter arrives at a station without a voter registration card, they are not turned away. A provisional ballot can be provided by the ballot database for use in this case. The nature of a provisional ballot allows it to only be used for common elections (i.e. statewide, and national). Even then it is only referenced in cases where an election is a closely contested count.

Voting Machine Details

Security

It is essential that a curtain surround the entire device. This curtain is to provide protection towards the privacy of the voter both physically and electronically. In the first case, it provides a visual barrier from allowing outside snooping towards what selections a voter is making. In the second case the curtain will use a material for the blocking of electromagnetic signals by being laced with strands of copper fiber. This provides a start towards preventing electronic interference snooping such as TEMPEST. Also, it is advised that the monitors used in these machines incorporated LCD screens rather than CRT to further protect against emanation monitoring attacks.

Handicapped Access

There will be a headphone jack on the front of the machine that is available for sightless or illiterate persons. These headphones will present a computer generated sound to the user.

The audio option will be provided on a per ballot basis. This audio sample quality does not need to be high quality. In the case of a statewide election (i.e. Washington's 49 districts) the audio sample can be included within a ballot's XML format giving each district ~14 MB for use (on a standard CDR).

Blind users will be able to properly vote without outside help via the headphones and the Braille numbering on the input buttons. Also included on the voting machine is a small electronic pad and pen, which may be used for write-in votes. After a write-in vote the system will echo back what characters it interpreted.

Alternatively, if a voting district decides against the pad and pen for financial reasons they may ask the hardware manufacturer to instead include a simple arrow controlled keyboard.

Tallying

Result Distribution and Tallying

We break all poll and tallying sites into a hierarchy with the state capitol at the root node, and local poll sites at the leaves (see fig. 1). Each entity has a physical presence somewhere in the state. We assign a unique number to each node at a given level in each subtree. At the bottom of the tree, poll sites collect votes from voters and tabulate local tallies. Sites keep tallies for their own elections, and pass their tallies for elections outside their jurisdiction up the hierarchy tree. Non-leaf nodes function like routers in the Internet: they forward tallies from one child in the tree to another, or from higher-level nodes down to their children.

The system is similar to that of the postal network, and not unlike an IPv4 network. The state can specify the use of this most generic tree structure, or a more customized topology, by shipping appropriately-configured routing tables with the rest of the election-day information that goes out to sites. Routing tables, like ballot information, are stored in XML files.

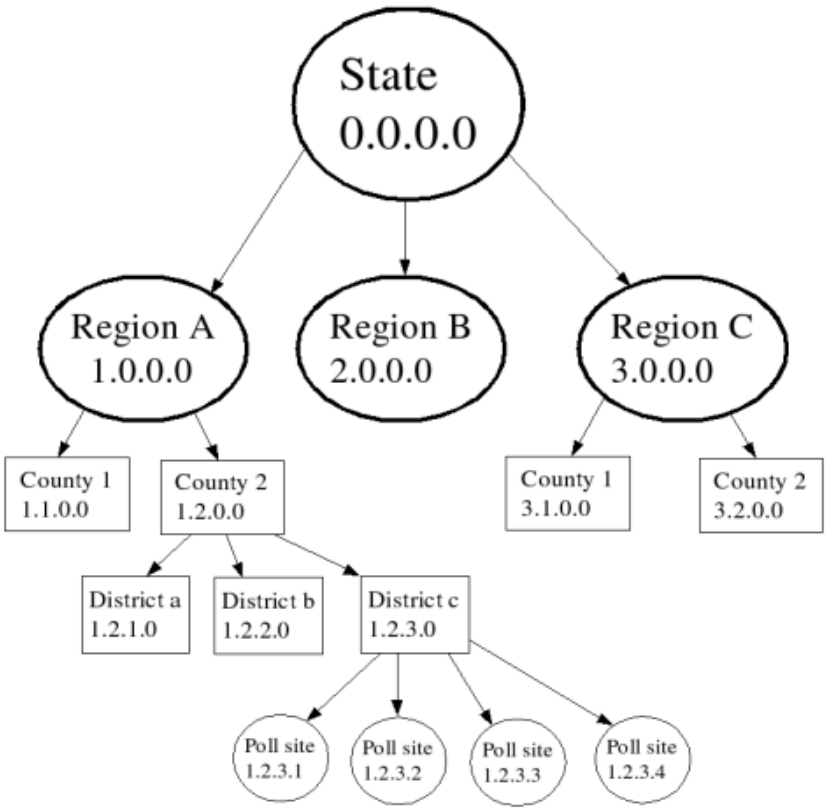

figure 1. A hierarchical, network view of the election system

Delivery Methods

We can not send the tally results through the Internet because of the risk of a denial-of-service attack. The most systems currently in use still rely on voice communication, but because the number of communications has increased we need further automation.

The similarity of our distribution network to the Internet offers many benefits to using an electronic system. Each node in the system will connect with a standard modem over the telephone network. If electronic transmission fails, sites fall back on using certified US mail to transfer XML data in printed hardcopy.

Tally Reporting Protocol

The calling node dials in to the receiver and sets up a PPP connection. Then the caller initiates an SSL 3.0 session, over which both ends authenticate themselves using certificates, and the caller sends one or more XML tally documents. After each document, the receiver ACK's or NAK's to indicate success or failure of its delivery. When the last document has been received, the caller closes the SSL session, then closes the PPP connection and hangs up.

Other References

TEMPEST relevant material:
Copper Mesh Purchasing:
http://www.twpinc.com/rfi.html

The Complete, Unofficial TEMPEST Information Page:
http://www.eskimo.com/~joelm/tempest.html

Appendix A

A Sample XML ballot DTD:

```
<?xml version="1.0"?>
<!DOCTYPE ballot [
        <!ELEMENT ballot    (office)>
        <!ELEMENT office    (position, region, candidate)>
        <!ELEMENT candidate         (name, party)>
        <!ELEMENT proposition (question)>
        <!ELEMENT position          (#PCDATA)>
        <!ELEMENT region    (#PCDATA)>
        <!ELEMENT name              (#PCDATA)>
        <!ELEMENT party     (#PCDATA)>
        <!ELEMENT audio             (#PCDATA)>
        <!ELEMENT hash      (#PCDATA)>
        <!ELEMENT signature         (#PCDATA)>
        <!ELEMENT question          (#PCDATA)>
]>
```

A Sample XML tally DTD:

```
<?xml version="1.0"?>
<!DOCTYPE tally [
        <!ELEMENT tally     (office)>
        <!ELEMENT office    (position, region, candidate)>
        <!ELEMENT candidate         (name, party, votecount)>
        <!ELEMENT proposition (question, answer, votecount)>
        <!ELEMENT position          (#PCDATA)>
        <!ELEMENT region    (#PCDATA)>
        <!ELEMENT name              (#PCDATA)>
        <!ELEMENT party     (#PCDATA)>
        <!ELEMENT votecount         (#PCDATA)>
        <!ELEMENT answer    (#PCDATA)>
        <!ELEMENT hash      (#PCDATA)>
        <!ELEMENT signature         (#PCDATA)>
        <!ELEMENT question          (#PCDATA)>
]>
```

A sample Routing Table XML DTD

```
<?xml version="1.0"?>
<!DOCTYPE routingtable [
        <!ELEMENT routingtable     (route)>
        <!ELEMENT route            (network, phonenumber)>
        <!ELEMENT network                  (#PCDATA)>
        <!ELEMENT phonenumber   (#PCDATA)>
]>
```

A Sample XML ballot File:

```
<!DOCTYPE root-element SYSTEM “sample.dtd”>
<?xml version=”1.0”?>
<ballot>
        <office>
                <position>President</position>
                <region>National</region>
                <candidate>
                        <name>George W. Bush</name>
                        <party>Republican</party>
                        <audio>president-bush-george-w.audio</audio>
                </candidate>
                <candidate>
                        <name>Al Gore</name>
                        <party>Democrat</party>
                        <audio>president-gore-al.audio</audio>
                </candidate>
        </office>
        <proposition>
                <question>Do you want new taxes?</question>
        </proposition
</ballot>
<hash>asdlhjk28dfh8292bdh28dwkj7wanh1h</hash>
```