A Solution for E-voting

The effectiveness of this proposed system lies in the unbreakable encryption device. A really concise and unified system must be done on line. The most recent CRS government reports on E-voting do not even consider on line voting. Here is a paragraph from that report.

> *Currently, five different kinds of voting technologies are used: hand-counted paper ballots, mechanical lever machines, computer punchcards (Votomatic and Datavote), marksense forms (also called optical scan), and direct recording electronic systems (DRE). The last three systems are computer-based. All systems except lever machines and DRE use document ballots on which the voter records choices. Punchcard systems are the most common, used by about one-third of registered voters, with marksense systems used by about one-quarter. In all but a few states, more than one kind of technology is currently in use.*

The most advanced system is the DRE. Most of those involved with the voting problem do not think of encryption to any significant degree because it is not vital to the operation of a DRE. Without foolproof encryption online systems are vulnerable. The proposed hardware encryption system is truly unbreakable. Most encryption systems are algorithmic and use primarily linear feedback shift registers. Algorithmic systems are then used to break them.

The proposed system does not use algorithms and so is impervious to such attacks. It is a truly unique system that cannot be broken. This allows the voting machine to be lodged anywhere there is an Internet connection. It will be safer than ATM machines (which are really quite safe) and extremely inexpensive to manufacture. Each voting machine is unique so even if one were to be compromised all the others devices would be unaffected.

The polling place may or may not contain storage or analytic software. It should basically be data transfer point, much as is an ATM device. When a person votes the voting kiosk delivers a print to the voter and transfers the results to a server. This server will be at the hub of the particular type of vote. Local elections will be stored and analyzed in the city or other local municipality, state elections at the state capitol and federal elections in Washington.

Each voting terminal will be a simple client machine that operates the kiosk. Each terminal will contain a version of the hardware encryption device. In this case the encryption device will only work on one machine. It would be useless to hack the terminal, as there is nothing there to hack. Both the terminal and the encryption module would need to be stolen and if that were to happen, since each terminal uses a unique encryption device, the server would only have to be notified that the stolen device was no longer valid.

The server would contain the duplicate of every encryption device in that particular voting system. The data from each individual terminal would be routed to the proper encryption module where the results would be decoded and tabulated. The results

would be up to date minute by minute and the final result would be known immediately when the polling place closed.

The printout the voter would receive is to a degree cosmetic. In the proposed system the redundancy is such that such a paper trial would most likely never be needed. One advantage to this proposed voting system is that the voter could change his or her vote up to the moment when the polls close. The use of printouts would compromise this advantage.

This entire system would be very inexpensive. The client machines would not need hard drives, as all storage would be on flash drives. Since the encryption device would be constructed in groups and the setup of the device would be designed by software absolutely no one would know the coding system of any device. Reverse engineering a single device would be pointless, as the device would have to be stolen in order to do this and once it was discovered missing it would be deactivated in the system.

The voter could be issued a card that would be much like a credit card. The voting terminal would only operate while the card is inserted or swiped. The card would contain sufficient data so as to identify the user and allow the server to determine if the card is reused.

The hardware of this voting system contains no moving parts. The component cost is so low that the triple redundancy that is used by the military would be very effective.

Procedure Flow

If magnetic stripe cards were not issued when the voter registers, an alternate method would be employed. Once the voter has been identified at the polling place a machine issues a card with a magnetic strip (much like those in a subway station). This strip contains a number linked with this voter. The voter enters the booth and insets the card. The card is swallowed and the data from the strip is read. The number is checked to verify that it has not been used before and the voting machine displays the touch screen with the selections.

Once the selection are made the screen displays the selections in list form:

President – Oscar Blodget
Vice President – Herman Schmiddle
Amendment 7 – yes
etc.

The voter can then correct any errors before the vote is saved.

Sound systems now exist that confine the audible sound to the area of the listener. It would be to great advantage if the voter could click on a routine that would verbally describe each article on the ballot. How many people really know what ‘amendment 7’ actually is?

When the voter accepts the selections the machine adds the selections and the code identifying the voting machine to the voter code number and prints a copy for the voter. Then the data is encrypted and stored in flash memory on the machine. The selection data and the data on the strip are erased. Simultaneously this encrypted data is

directed to flash memory on a master device in the polling place. At the same time the data is sent to the server that will count the votes and stored the result in flash memory. This result is also stored on a device at the State or City judicial center. It is also stored at the headquarters of the participating political parties and any others that might be desired.

Only the actual voting machine has the hardware encryption device. When the polls close all of the flash memories are fed to storage devices. This will provide a half a dozen or more simultaneous permanent records of the votes. The decryption device will reside on the computer that will count to votes. The encryption/decryption devices are very small so the decryption device would hold a decoder for every voting machine. All of the stored data are compared to prevent tampering. The votes are then decrypted and automatically counted. Another machine or two could have decryption devices to verify the count.

This would ease the congestion at polling places as such places would only need to exist primarily for handicapped persons and those who might have lost their voting card. Since the voting machines could be placed anywhere, voting would just as easy overseas as domestically. The terminals could be located at embassies, military bases and other similar locations. The absentee ballot would virtually disappear.

Since this system is based on the EPROM the actual hardware is comprised of very simple off-the-shelf components. They could safely be manufactured anywhere. So as not to further alarm the voting population they should likely be assembled and programmed in the US.

A voting unit would be comprised of a device console that is used to cast the vote and a the necessary storage devices These components are all exactly alike and do not become part of the system until they are programmed.

The actual programming of the sets would be done in a government facility with all of the necessary protective measures. A voting console and its memory systems are all programmed in a batch and numbered as a set. The voting console is sent to a poling center and the chips to the various organizations as desired.

When the voter registers he or she is sent a card similar to an ATM card. The voter selects a password. When he or she votes it is only necessary to swipe the card and enter the password.

All registered voters are in a main database (relational). Use of such a database means that a voter can cast his or her vote anywhere in the world. The database would be checked to see that the voter was not attempting to vote more than once for the same issue. The software would only allow votes that are legal within the residence of the voter regardless of where the voter is casting the vote. Only these choices would appear on the kiosk display.

This would do away with the need for most absentee voting as, since the voting console is very inexpensive, it could be easily shipped in quantity and operated anywhere in the world. If a voter is away from his or her district but wished to vote for a district issue there would be no problem.

Summary

Because of the very low cost of the device it could be sold (or issued at cost) to individual users so that a voter could vote from his or her own home. This would bring the one person – one vote reality much closer. There are already movements so do away with the Electoral College. Here is a quote from an article by Jamie Raskin, a Maryland state senator and a professor of constitutional law at American University's Washington College of Law.

> *Public opinion polls have long shown that upwards of 65 percent of Americans favor a direct national popular vote for president in which all of our votes count equally. The puzzle has been how to reconcile a national popular election with the antique mechanics of the Electoral College, which Thomas Jefferson called "the most dangerous blot on our Constitution."*
>
> *But now the state of Maryland has taken a bold and creative step to show how it can be done. On April 10, 2007, Maryland Governor Martin O'Malley signed into law a plan to have Maryland enter and launch an interstate compact in which all member states agree to cast their Electoral College votes for the winner of the national popular vote. The agreement takes effect when it is enacted by a number of states representing a majority of electoral votes (270).*

Those without computers access could vote at libraries, post offices and many other suitable locations. The reason it would work and be perfectly safe is the redundancy of the system and the unbreakable encryption device.

Thomas Wagner
May 2007