

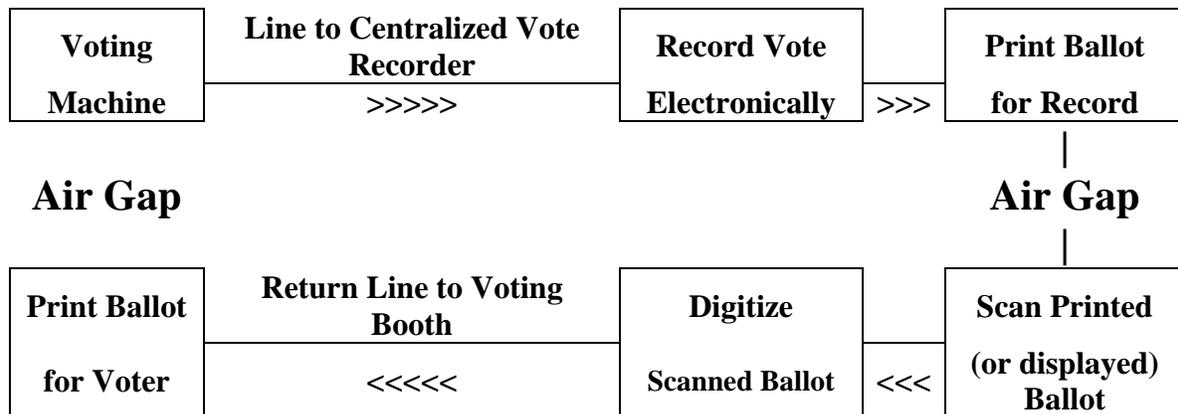
Voting Security

The key to **creating voter trust** and maintaining security against voting fraud is to use the same two fundamental methods that are used for high-security computer systems - an **air gap**, and **separation of control of incoming and outgoing data**.

High security systems do not allow outside direct access to the core of the system. Data is input directly either from a keyboard or from intermediate media (CD, tape, etc) that has been scrutinized when not under the control of the originating system. For high security communications, the incoming and outgoing communication paths are kept separate and monitored to detect attempts to control both paths simultaneously. Systems that don't use air gaps will always be vulnerable to electronic tampering and will never be **fully trusted by the voters**.

Secure voting can be accomplished with off-the-shelf technology using the techniques of air gaps and separate communication paths.

Below is an outline of the protocol:



1. Each voting station is equipped with two basic laptops, one printer, a broadband internet connection, and a phone line.

One laptop would be used for transmitting the vote, and the other for receiving confirmation of the vote.

These could be the "\$100 laptops" currently being produced for distribution to third-world children, or laptops provided by donors for the purpose of public relations and that would be subsequently donated to local schools. The same could apply to the printers.

Each laptop would be prepared by erasing and reformatting the hard drive, and installing an open operating system such as Linux and open internet communication

software such as Firefox. The vote transmission laptop would have internet connection and point-&-click balloting software installed. The vote confirmation laptop would have phone line connection and printing software installed. There is no connection between the two laptops. More intensive security measures should be considered, such as tests to detect hardware viruses or other tampering not eliminated by standard erasing and reformatting procedures.

2. Each ballot is transmitted via the internet to a central certified secure vote recording facility.

Freely available or donated software would record the votes and also monitor the incoming signal for signs of tampering and take the appropriate action.

3. Each incoming ballot is printed or otherwise visibly displayed at the recording facility.

One might envision a system similar to a high-speed newspaper printing press. The volume of ballots might make real-time physical printing unfeasible - this needs to be determined. If feasible, the use of an existing press might be donated by a newspaper for the purpose of public relations. If physical printing is not feasible, each incoming ballot would be displayed on a monitor at the recording facility and scanned from the display.

4. The printout or display of each incoming ballot is scanned by a system not connected to the incoming system.

This is the air gap. Scanners have become relatively inexpensive, and could also be donated for subsequent donation to local schools. Standardization of ballot formats would simplify the scanning software requirements and speed up the entire process by allowing a text scan/print rather than an image scan/print.

5. The scanning system digitizes the scanned ballot and transmits it via the phone line connection to the confirming laptop, where two copies are printed (one for the voter, one for the precinct).

The confirmation signal would also be monitored for signs of tampering. The separation of the signal paths would require perpetrators to simultaneously control both the transmission signal and the confirmation signal, which in itself should be sufficiently difficult that the voting system could be expected to remain secure.

Cost of components: Initially the number of voting stations would be virtually the same as the current number of voting stations, and each voting station would require the same set of components as described below, ideally with the components being donated by manufacturers or other parties for later distribution to schools. Each polling station could be set up by volunteers according to established standards, and then each station would be certified by traveling teams of reviewers (as I assume they are currently). While some

polling stations may need inexpensive temporary wiring and adapters to multiplex the use of multiple stations over single phone lines and internet lines, polling stations in schools could be generally expected to have the necessary capacity in place. In fact, setting up and running voting stations would be a great civic and computer science project for middle and high school students every year. Such stations could be maintained effectively full time not only for official elections but for secure public opinion polls as well.

Timing: The system would be composed entirely of available off-the-shelf software and hardware, and could be put in place very quickly. The first step would be to establish minimum standards for the hardware and software at the polling stations and the ballot recording facility, followed by a campaign to solicit donors and volunteers, if not directly and immediately funded by the State.

The future: As the public becomes familiar and comfortable with the concept of secure voting using air gaps and separation of communication paths, it would be expected that online voting would substantially replace voting in person at a poll station, allowing reduction in the number of physical stations required. The separation of paths for online voting would be in the form of a confirming email that is transmitted by an internet path that is electronically verified to be sufficiently separate from the ballot transmission path to ensure that both paths cannot be simultaneously controlled by any perpetrator for the purpose of altering a statistically significant number of votes. This would also enable real-time polling on a wide variety of issues and reduce the ability of special interests to claim greater support for their agenda than actually exists. This would also enable voters to have access to thoughtful pro and con consideration of issues at a central resource well in advance of an election, instead of basing their vote on sound bites, biased media offerings, and brash conflicting claims in State-issued voter pamphlets. While it may not be realistic to expect that an extremely high number of eligible voters would devote sufficient time to fully understand the issues, it can be expected that a high proportion of those who actually vote would do so.

We have the opportunity and the responsibility to lead the way to elimination of voting fraud nationwide and ultimately worldwide, and changing apathetic or repressed societies into involved societies.

Please use these ideas in any way that you find useful.

Ben Goodman
Palo Alto, CA