Open Source Voting

Arthur M. Keller, Ph.D.
David Mertz, Ph.D.
Outline

- Concept
- In-Precinct Architecture
- Central Architecture
- Current Status
- Rollout Plan
- Privacy Issues
- Voter-Verifiable Audit Trail
- Conclusion
Concept

• Secret Ballots Talled in Public incompatible with Voting Machines and Tabulators whose inner workings are Trade Secrets

• Open Voting Consortium created to promote Public Software for Public Elections
In-Precinct Architecture

- Voter Signs In
- Voter Makes Selections on Electronic Voting Machine
- EVM Prints Ballot
- Ballot
- Voter Verifies Ballot
- Blind or Reading-Impaired Voter Verifies Ballot
- Voter Casts Ballot by Placing in Ballot Box
- Paper Ballots are Tallied and Reconciled with Electronic Audit Trail
- Electronic Audit Trial (Transferred When Polls Close)
Sample Ballot
Central Tabulating System

- Reliable, secure, auditable voting machines are not enough.
- We also need reliable, secure, auditable canvassing (counting) systems used centrally.
Central Architecture

Results from Precincts -> Central Tabulator

Bulk (Optical) Ballot Scanner

Paper Ballots

Central Tabulator -> Unofficial Results (Periodically after polls close)

Unofficial Results Web Server

Election Management System

Internet Display of Unofficial Results

Internet
Current Status

- Prototype built of precinct-based system.
- Demonstration covered on TV, radio, and newspapers.
Rollout Plan

- Develop prototype of central tabulator.
- Develop production version of central tabulator, election management system, and reporting systems.
- Develop production quality version of central optical scan ballot reader.
- Develop production quality version of precinct-based optical scan ballot reader.
- Develop OVC Electronic Ballot Printer system.

- Options: retrofit existing electronic voting hardware to use OVC Electronic Ballot Printer software.
- Eases adoption and saves money at cost of some security risk (far, far less than existing systems).
Privacy Issues

- Open Source (published source, so anyone can inspect to ensure no hidden trap doors or covert channels).
- Secret ballot (voter must disclose identity but ballot must not identify voter). Potential risks of voting token.
- Printed ballot and Privacy Folder.
- Barcodes.
- Blind and reading-impaired voters.
- Languages.
- Random ballot IDs.
- Public vote tallying.
- Reporting results by precinct.
- Privacy and voter collusion (printed ballot ID, write-ins).
Voter-Verifiable Audit Trail

- Helps ensure electronic ballot image is correct.
- Useful for recounts.
- Useful for audits (*if* and *when* they are done!)
- If not machine readable and tallyable, will be effectively used *only* when legally required.
- Reel-to-reel approach compromises voting privacy by maintaining order of ballots.
- ATM-style roll hard to count by machine.
- Use of airline-style cards could solve these problems by using known reliable printers.
Conclusion

- Give election officials more choices.
- Enable best-of-breed voting systems.
- Enable competition in services and follow-on support.
- Build open source voting systems vendors can adopt.
- Cheaper, more reliable and secure, auditable, and more trustworthy.
- Privacy should be added to evaluation standards along with reliability, security, and trustworthiness.
For More Information

- See papers and talks at http://www-db.stanford.edu/pub/keller and click on “Electronic Voting.”
- Join the Open Voting Consortium at http://openvoting.org
- And contact Alan Dechert alan@openvoting.org to volunteer.