Open Source Voting
Arthur M. Keller, Ph.D.
David Mertz, Ph.D.

Outline
- Concept
- Fully Disclosed Voting Systems
- Open Source Voting Systems
- Existing Open Source Voting Systems
- Open Source Is Not Enough
- Barriers to Open Voting
- What’s Wrong with DRE Voter-Verifiable Audit Trail
- New System Ideas
- Conclusion
- What You Can Do
Concept

- Secret Ballots Tallied in Public
- *incompatible with*
- Voting Machines and Tabulators
- whose inner workings are Trade Secrets

Concept

- **Wholesale Fraud versus Retail Fraud**
  - *Long and ignoble history of ballot tampering*
  - A ballot box contains *hundreds* of potentially vulnerable votes
  - A DRE voting system affects *millions* of potentially vulnerable votes
Concept

- **Computer + Human = Better than Just Human**
  - Computer voting systems do not substitute for human procedures, but enhance the capability of people to conduct fair elections
  - Under the right arrangements, corrupt officials are unable to corrupt elections
  - The nature(s) of trust

Fully Disclosed Voting Systems

- Part of making the entire voting process open to full inspection by the public
  - Inventory of components
  - Full source code (except true COTS)
  - Object code images
  - Checksums of object code images
  - Hardware, Software, System Specifications
  - Documentation
  - Internal and external document formats and samples
  - Hardware dependencies, specifications, and requirements
  - For COTS: specifications, requirements, uses, version numbers, dates of manufacture
  - Feature checklists
  - License(s)
  - Reports on non-internal tests
  - Procurement contracts
Open Source Voting Systems

- Increases security and reliability
  - Often secrecy of existing systems is to avoid embarrassment
  - Open source systems are designed to be secure without secrecy
  - “Security by obscurity” is not true security
  - Many eyes can find bugs, errors, or fraud
  - Open source systems (e.g., Linux, Apache) often more secure than comparable secret source systems (e.g., Windows, IIS)

- Differences (compared with other Open Source applications)
  - Special purpose application
  - Difficulty in recruiting volunteers
  - Security needed in changing source code
  - Hard to finance
  - Freedom to test, experiment, and analyze

Existing Open Source Voting Systems

- OVC Prototype System
  - Described last year
  - Demonstrated in 2004
  - Advanced the debate about voting systems
  - Not a production quality system

- Berkeley research project (Yee, Wagner, et. al)
  - Demonstrated in 2006
  - Similar in both features and limitations to OVC Prototype

- Open Voting Solutions
  - A full, production-quality open source voting system
  - Awaiting certification (an expensive process)
  - Derived from OASIS EML open source voting tools and components

- Non-US Systems
  - Australian Capital Territory system
New Open Source Voting Systems
VoComp 2007–Univ. Voting Systems Competition

- **Punchscan**
  - End-to-end verified system with encryption
  - Two-part ballot with receipt
  - Cannot manually recount
  - First place at VoComp 2007

- **Prêt à Voter**
  - End-to-end verified system with encryption
  - Two-part ballot with receipt
  - Cannot manually recount
  - Supports Ranked Preference Voting (such as IRV and STV)
  - Second place at VoComp 2007

- **Prime III**
  - DRE with video backup

- **Voting Ducks**
  - Coercion-free Verifiable Internet Voting
  - Uses credentials mailed and submitted by cell phone

Open Source Is Not Enough

- **Other parts of voting process must also be disclosed**
  - Adequate audits
  - Paper ballots (whether hand marked or machine marked or printed)
  - Public right of access and public right to observe entire process
  - Timely disclosure to enable recounts and contesting results
  - Electronic disclosure in any medium in which the records are readily available
  - Electronic disclosure in any format to which data is readily convertible with the data custodian’s existing software
  - Usable format (e.g., not fragmented)
  - Disclosure costs only actual cost of materials (not labor)
Barriers to Open Source Voting

- High cost of system certification
- Entrenched relationships with existing vendors
- Experience of existing vendors
  - Trust by election officials
- Limited market
- Risk of insertion of fraudulent code
  - Problem with pure volunteer development
- Trust by elections officials at odds with trust by the voting public
  - Elections officials motivations are different
  - Most elections departments are small and understaffed

What’s Wrong with DRE

Voter-Verified Audit Trail

- Helps ensure electronic ballot image is correct.
- Useful for recounts.
- Useful for audits (if and when they are done!)
- Limited accessibility.
- 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.
- Better: Voter Verified Paper Ballots directly counted for each election.
New System Ideas

• Hand-marked optical scan paper ballots
• Electronic Ballot Printer for accessibility
  - Audio or Video interface
  - Prints an entire optical scan paper ballot compatible
  - with hand-marked ones
• Precinct-count optical scanner and voter ballot verifier
  - Scans ballot (and saves image)
  - Examines image to determine location of marks
  - Interprets mark locations to create an Electronic Ballot Record
  - Displays (or speaks) ballot choices to voter
  - Voter verifies choices or ejects paper ballot for correction
  - If voter verifies ballot is read correctly, non-sequential serial
    number printed on ballot and written on images
• Scanner totals posted at precinct and available from web
• Ballot images available from precinct on CD-R
  - In random order by serial number
• Enables ballot-by-ballot auditing
• Let’s change the debate, again

New System Ideas (continued)

• Publish images of all ballots on CD-R or DVD-R
  ✓ By batch (e.g., by precinct (or scanner) for “regular” ballots)
  ✓ Each ballot image accompanied by corresponding Electronic
    Ballot Record
  ✓ With vote tallies for each batch
  ✓ Enables ballot-by-ballot auditing
  ✓ Can be matched with overall vote totals (and batch totals)
  ✓ Can be matched with precinct tallies posted at close of voting
  ✓ Allows complete hand-counting by the public
  ✓ Privacy issues with stray marks, problem reduced by electronic
    ballot printers
  ✓ Allows third-party vote auditing and tallying software
  ✓ Good opportunity for open source, volunteer contributed code
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.

What You Can Do

- Current legislative status: HR-811; California FOSS Voting Resolution
- For more information, see papers and talks at http://infolab.stanford.edu/pub/keller and click on “Electronic Voting.”
- Contact your election officials (county, Secretary of State).
- Contact your elected officials (federal, state, and county).
- Help with new prototype system (new ideas section).