Privacy Issues in an Electronic Voting Machine

Arthur M. Keller
UC Santa Cruz and Open Voting Consortium

David Mertz
Gnosis Software

Joseph Lorenzo Hall
UC Berkeley

Arnold Urken
Stevens Institute of Technology

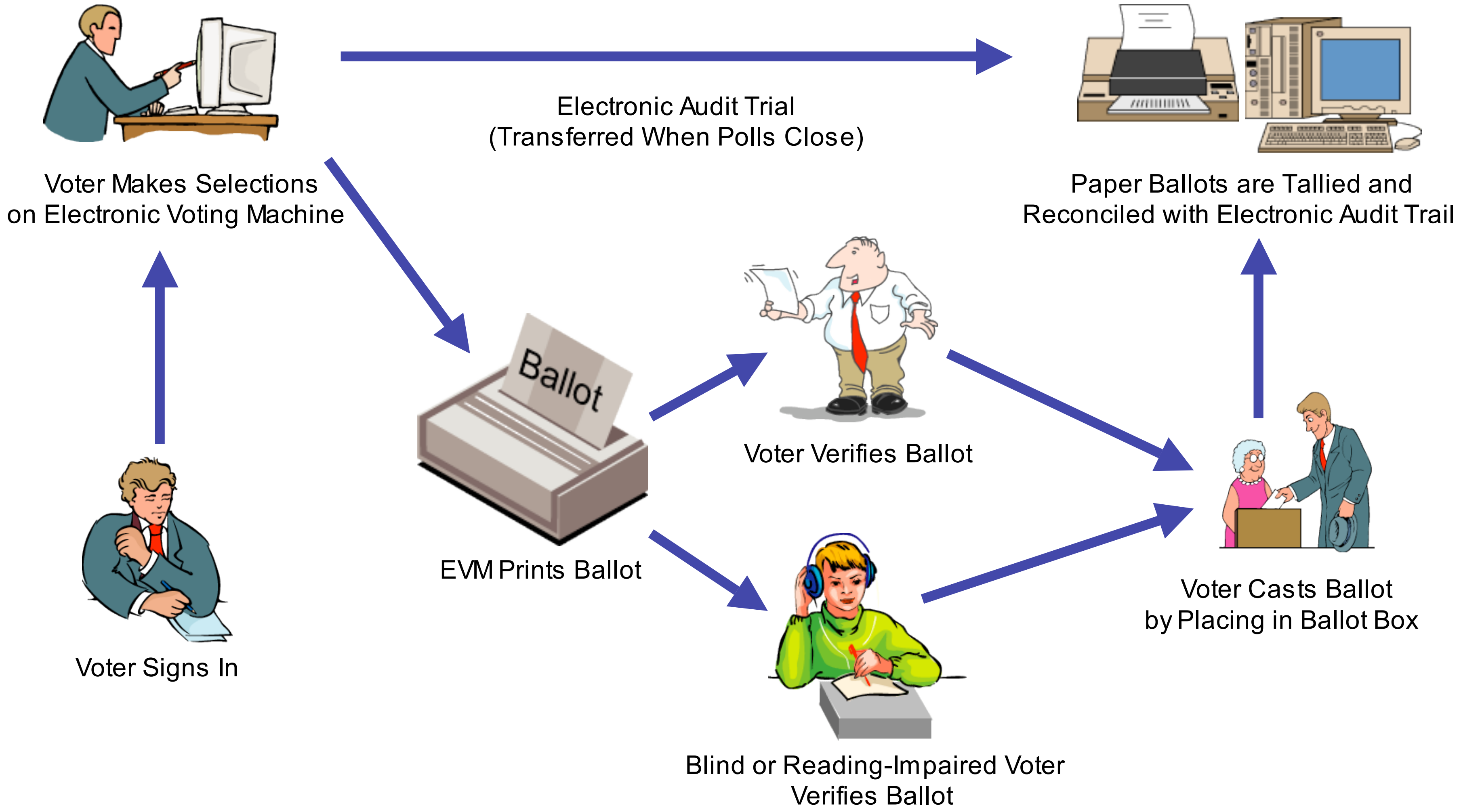
Outline

- Secret ballot
- OVC approach
- Privacy Issues
- Conclusion

Secret Ballot

- Ballots cast in secret.
  And tallied in public.
- Voter must disclose identity.
  But ballot must not identify voter.
- No covert channel.
- No link between registration data and ballots.

OVC System



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

Open source

- Published source, so *anyone* can inspect to ensure no hidden trap doors or covert channels.

Voting token

- Allows voter to vote and specifies ballot type.
- Depending on type of token, could compromise privacy of voter identity.
- More problematic with electronic voter sign-in system.

Printed ballot and privacy folder

- While voter walks around polling place, voter-verified paper ballot can be seen by others.
- Folder that hides the human readable portion of ballot, but shows the barcode.

Reading-impaired interface

- Allows blind or reading-impaired voter to cast a ballot.
- Prints a ballot just like ordinary electronic voting machine.

Barcodes

- Facilitates electronic tallying of ballots.
- Facilitates blind or visually-impaired voter to verify ballot audibly.

Ballot verification station

- Allows blind or reading-impaired voters to “hear” their choices, and therefore verify their paper ballots.

Languages

- Potentially compromises privacy of votes for non-English speakers.
- Solution: Always print a non-English language, either voter’s language or a random one.
- Solution might not work with preprinted ballots (such as *fill-in-the-bubble* or *connect-the-lines).*

Random ballot IDs

- Helps reconcile paper ballot against electronic audit trail.
- Electronic audit trail maintained in ballot ID order, *not* order ballot was printed.

Public vote tallying

- Ballot box should be shuffled before anyone can see the printed ballots, otherwise vote order apparent.
- OVC reconciles paper ballot and electronic audit trail.
- A problem for Direct Recording Electronic voting machines.

Results by precinct

- Display results by precinct at polling place and on county website.
- Separate by in-polling place regular ballots, and all other ballots (absentee, provisional).
- Small numbers of *other* ballots might compromise privacy. So *tallies* of other ballots are combined, but *counts* are kept separate.
- Good to allow a voter to determine whether absentee or provisional ballot was counted or rejected, and if not, why not.

Privacy and voter collusion

- Printed ballot ID can compromise privacy.
- Write-in votes can compromise privacy.
  - Vote for yourself.
  - Especially a problem when *all* ballots are displayed individually online.
  - Why some jurisdictions limit write-in votes to *only* declared candidates.

Voter-verifiable audit trail

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

Conclusion

- Privacy in electronic voting systems is a problem requiring analysis and study.
- Should be added to evaluation standards along with reliability, security, and trustworthiness.
- Our study in the context of the OVC system, and many of issues applicable to other electronic voting systems.