Privacy Issues in an Electronic Voting Machine

Arthur M. Keller
UC Santa Cruz, Baskin
School of Engineering
Santa Cruz, CA 95066
+1(831)459-1485
ark@soe.ucsc.edu

David Mertz
Gnosis Software, Inc.
99 2nd Street
Turners Falls, MA 01376
+1(413)863-4552
mertz@gnosis.cx

Joseph Lorenzo Hall
UC Berkeley, SIMS
102 South Hall
Berkeley, CA 94720
+1(510)642-1464
joehall@berkeley.edu

Arnold Urken
Stevens Inst. of Technology,
Political Science
Hoboken, NJ 07030
+1(201) 216-5394
aurken@stevens.edu

ABSTRACT

In this paper, we describe the Open Voting Consortium's voting system and discuss the privacy issues inherent in this system. By extension, many of the privacy issues in this paper also apply to other electronic voting machines, such as DREs (Direct Recording Electronic voting machines). The privacy issues illustrate why careful and thorough design is required to ensure voter privacy and ballot secrecy.

Categories and Subject Descriptors: K.4.1 [**Computers and Society**]: Public Policy Issues — *privacy.*

General Terms: Design, Human Factors, Legal Aspects.

Keywords: Electronic voting, open source, privacy design.

1. INTRODUCTION

The requirements for secrecy in elections depend upon the values and goals of the political culture where voting takes place. Gradations of partial and complete privacy can be found in different cultural settings. Most modern polities institutionalize the ideal of complete privacy by relying on anonymous balloting.

The use of secret balloting in elections — where a ballot's contents are disconnected from the identity of the voter — can be traced back to the earliest use of ballots themselves in 6th Century B.C.E. Athens, Greece. The public policy rationales for instituting anonymous balloting typically aim to minimize bribery and intimidation of the voter [1]. Secret ballots, although not always required, have been in use in America since colonial times. Today, almost one hundred years after most states in the U.S. passed laws to require anonymous balloting, a strong sense of voter privacy has emerged as a third rationale.

These cultural values and practices contribute to the sets of user requirements that define the expectations of voters in computer-mediated elections and determine alternative sets of specifications that can be considered in developing open source software systems for elections [7]. The Open Voting Consortium (OVC) has developed a model election system that aims as one of its goals to meet these requirements. This paper describes how the OVC model ensures ballot privacy.

The OVC has developed the model for an electronic voting system largely in response to the reliability, usability, security, trustworthiness, and accessibility concerns of other voting systems. Privacy was kept in mind throughout the process of designing this system. Section 2 of this paper discusses the requirements for a secret ballot in more detail and how secrecy could be compromised in some systems. Section 3 describes how the OVC handles the privacy concerns. While this paper focuses mostly on privacy issues for US-based elections, and how they are addressed in the OVC system, many of the issues raised are applicable elsewhere.

2. SECRET BALLOT REQUIREMENTS

The public policy goals of secret balloting — to protect the privacy of the elector and minimize undue intimidation and influence — are supported by federal election laws and regulations. The Help America Vote Act of 2002 [5] codifies this as "anonymity" and "independence" of all voters, "privacy" and "confidentiality" of ballots and requires that the Federal Election Commission create standards that "[preserve] the privacy of the voter and the confidentiality of the ballot."

The Federal Election Commission (FEC) has issued a set of Voting System Standards (VSS) [4] that serve as a model of functional requirements that elections systems must meet before they can be certified for use in an election. The FEC VSS state explicitly:

"To facilitate casting a ballot, all systems shall: […] Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual State law;" ([4] at § 2.4.3.1(b).)

This high level requirement of not exposing any information about how an individual voted is required of all voting systems before certification.

It is not sufficient for electronic voting systems to merely anonymize the voting process from the perspective of the voting machine. Each time a ballot is cast, the voting system adds an entry to one or more software or firmware logs with a timestamp and an indication that a ballot was cast. If the timestamp log is combined with the contents of the ballot, this information becomes much more sensitive. For example, it can be combined with information about the order of votes cast collected at the polling place with surveillance equipment — from cell phone cameras to security cameras common at public schools — to compromise the confidentiality of the ballot. As described below, system information collected by the voting system should be kept separated from the content of cast ballots and only used in conjunction by authorized, informed elections officials.

Rebecca Mercuri proposed that Direct Recording Electronic (DRE) voting machines have a paper audit trail maintained under glass, so the voter does not have the opportunity to touch it or change it. [6] Some vendors are proposing that paper from a spool be shown to the voter, and a cutter releases the paper audit trail piece to drop into a box for safekeeping. [2] A challenge is to make sure that all of the paper audit trail is readable by the voter, doesn't curl away out of view, and yet the paper audit trails from previous voters is obscured from view. However, the paper audit trail can fall in a more-or-less chronologically ordered pile. The

WPES'04, October 28, 2004, Washington, DC, USA.
Copyright 2004 ACM 1-58113-968-3/04/0010...$5.00.

problem of reconciling the paper audit trail with the electronic ballot image is difficult to do in an automated manner if the paper audit trail cannot be sheetfed. Another approach is to keep the paper audit trail on a continuous spool. [7] While this approach has the potential to be more easily scanned in an automated fashion for recounts, privacy is compromised by maintaining the chronological order.

In the longer version of this paper, we discuss in more detail these issues. We discuss that problem that the voter's secret identity must be disclosed to poll workers and yet not be discernable from the ballot. Covert channels can be used to transfer identity of the voter to the ballot. A critical example is when the machine that prepares for the voter an authorizing token also contains the voter registration data, which might be passed to the electronic voting machine through that authorizing token.

3. SECURITY, PRIVACY, RELIABILITY

In the full version of this paper, we discuss a variety of issues and their solutions in security, privacy, and reliability for the voting system designed by the Open Voting Consortium and described more fully there.

Some of these issues are the following.

The Advantage of Free and Open Source Software. When the system is a black box, where the source code is maintained as a trade secret, we must trust the official testers. A frequent criticism of free and open source software is that, while the code is available for inspection, no coordinated inspection is actually conducted. [3] The absence of Non-Disclosure Agreements and restrictive intellectual property agreements encourages the large body of open source developers to inspect the code.

Randomization of Ballot-IDs. Under the OVC design ballots carry ballot-IDs to enable auditing of official paper ballots against unofficial electronic ballot images. Ballot IDs are easily remembered and can be a vehicle for disclosing the vote.

Privacy Issues with Barcodes. The Open Voting Consortium system design uses a barcode to automate the scanning and tallying of paper ballots. Such barcodes raise several possibilities for introducing covert channels.

Privacy in the Voting Token. The token given to the voter to enable her to use the electronic voting machine might contain information that could compromise anonymity. Analysis of the software and the poll worker interface for encoding the voter token can show the type of information that can be encoded.

Information Hidden in Electronic Ballot Images and Their Files. The electronic ballot images (EBIs) are stored on the electronic voting machine where the ballot was created. Storing the EBIs in a database management system can record sequence information that can be used to identify voters. Flat files can include the date/time in the file directory, a potential privacy risk.

Reading Impaired Interface. It is important that the ballot not record that the voter used the reading impaired interface. Nor should the electronic voting machine maintain such information in a way that identifies specific ballots. If a separate reading impaired voting station is used, the ballot-ID should be generated in a manner that does not identify the voting station used.

Printed Ballot. The secrecy of the voter's selections is at risk while the voter carries the paper ballot around the polling place. We use a privacy folder — an ordinary manila folder trimmed along the long edge so that the barcode sticks out.

Ballot Validation Station. The ballot validation station allows visually impaired voters, or anyone, to hear through headphones and therefore validate their paper ballots. Ballot-IDs should not be persistently stored by the ballot validation station.

Languages. Steve Chessin identified a problem with ballots for non-English speakers when printed in the voter's own language. This approach makes bilingual ballots easy to identify, and that can compromise ballot anonymity if only a small number of voters in a given precinct choose a particular language.

Public Vote Tallying. It is important that the ballots be shuffled before publicly visible scanning occurs. The ballots will naturally be ordered based on the time they were placed in the ballot box. The sequence of voting is a potential privacy risk.

Results by Precinct. Care must be taken to ensure that results posted by precinct do not compromise privacy and yet can be reconciled against county totals.

Privacy in the Face of Voter Collusion. Complex cast ballots, taken as a whole, contain potential covert channels.

4. CONCLUSION

We have discussed the privacy issues inherent the Open Voting Consortium's voting system that includes a PC-based open-source voting machine with a voter-verifiable accessible paper ballot. By extension, many of the privacy issues in this paper also apply to other electronic voting machines, such as DREs (Direct Recording Electronic voting machines). The privacy issues illustrate why careful and thorough design is required for voter privacy. Imagine how much work is required to ensure that such systems are secure and reliable.

Further information about the Open Voting Consortium can be found at http://www.openvotingconsortium.org. This paper is an extended abstract; a longer version may be found at http://www-db.stanford.edu/pub/keller.

5. ACKNOWLEDGMENTS

We acknowledge the work of the volunteers of the Open Voting Consortium who contributed to the design and implementation we describe. In particular, Alan Dechert developed much of the design and Doug Jones provided significant insights into voting issues. The demonstration software was largely developed by Jan Kärrman, John-Paul Gignac, Anand Pillai, Eron Lloyd, David Mertz, Laird Popkin, and Fred McLain. Karl Auerbach wrote an FAQ on which the OVC system description is based. Amy Pearl also contributed to the system description. Kurt Hyde and David Jefferson gave valuable feedback. David Dill referred some of the volunteers.

6. REFERENCES

[1] Albright, S. *The American Ballot*. American Council on Public Affairs, Washington, D.C., 1942.

[2] Avante VOTE-TRAKKER™ EVC308-SPR, http://www.aitechnology.com/votetrakker2/evc308spr.html.

[3] Cohen, F. Is Open Source More or Less Secure? *Managing Network Security*, *2002,* 7 (Jul. 2002), 17–19.

[4] Federal Election Commission. *Voting System Standards.* Vols. 1 & 2 (2002), http://www.fec.gov/pages/vssfinal/

[5] Help America Vote Act, 42 U.S.C.A. §§ 15301 – 15545.

[6] Mercuri, R. A Better Ballot Box? *IEEE Spectrum Online*, October 2, 2002, http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html

[7] Sequoia Voting Systems, "Sequoia Voting Systems Announces Plan to Market Optional Voter Verifiable Paper Record Printers for Touch Screens in 2004," http://www.sequoiavote.com/article.php?id=54

[8] Urken, A. B. Voting in a Computer-Networked Environment. In *The Information Web: Ethical and Social Implications of Computer Networking*, Carol Gould (ed.), Westview Press, Boulder, CO, 1989.