

Combining End-To-End Voting With Trustworthy Computing for Greater Privacy, Trust, Accessibility, and Usability (summary)

Russell A. Fink¹ and Alan T. Sherman²

August 9, 2009 (revised September 25, 2009)

Abstract. We advocate combining *Trustworthy Computing (TC)* techniques—including *Trusted Platform Module (TPM)* protocols, application attestation, and reduced software footprints—with *end-to-end (E2E)* technologies, to provide voter and universal verifiability while enhancing privacy, accessibility, and usability through trustworthy electronic systems. Current voting approaches with paper, electronic, and *end-to-end (E2E)* cannot meet every voting system requirement without using software to achieve greater efficiency, usability, and accessibility. But untrustworthy software systems can be compromised leading to disclosure of voter privacy or integrity—even in software-independent verifiable systems. TC techniques can bolster E2E systems through ensuring the correct software is running and managing cryptographic keys securely, thereby enhancing privacy, deterring confusion, detecting problems sooner, and making possible high-assurance electronic accessibility interfaces including for the blind. We analyze specific benefits that TC can bring to E2E systems such as Scantegrity II.

1 Introduction

Software independent integrity in E2E is so strong that some people think that E2E voting systems cannot benefit from TC computing platforms. While integrity problems (*e.g.*, swapped votes) can be eventually detected in E2E systems, problems are concealed until late in the game after the polls close and results are published. TC can eliminate or detect earlier some of these problems that occur in the polling place. Additionally, malicious software on an E2E system can easily violate voter privacy in a way that can never be detected. For example, in Scantegrity II [Cha08], malicious printer software could expose ballot codes and destroy voter privacy. Malicious scanner software could identify voters with stray marks, enabling coercion. Similarly, a compromised VoteHere touch screen could respond to a pattern of touches to disclose all votes received to that point. Thus, current E2E voting designs are neither immune to privacy attacks, nor quick at catching integrity problems (*e.g.*, in the polling booth).

Malicious software can also sow confusion and undermine public confidence in the election outcome, for example, through presentation attacks (*e.g.*, misreading voter inputs) and discrediting attacks (*e.g.*, planting fabricated evidence of fraud). Malicious code can also reduce system availability and reliability.

Despite the risks, all E2E voting systems rely on software to help print ballots, store and forward results. Software is also needed to provide flexible user interfaces allowing the physically disabled to cast votes unassisted. Voting systems that avoid computing technology suffer diminished usability and accessibility, despite that usability is the main problem of modern voting systems as witnessed by confusing butterfly ballots in the 2000 U.S. Presidential election. Scantegrity II lacks a trustworthy receipt printer, making everyone manually record numerous codes in lengthy races. Without an electronic interface, Scantegrity II currently impedes the visually impaired.

TC benefits E2E by enabling good usability and by providing defense in depth—securing distinct aspects of the voting system similarly to how a computer networking stack is secured in layers. To realize these benefits, however, we must understand what features are enabled by TC, and where to apply TC in an E2E architecture.

For more details, see our position paper [Fin09b], which includes a sketch of how to add TC to Scantegrity II. In our companion paper [Fin09a], we propose a more secure design of *Direct Recording Equipment (DRE)* using *Trusted Platform Modules (TPMs)*.

¹ Russell A. Fink, Johns Hopkins University / Applied Physics Laboratory, 11100 Johns Hopkins Road Laurel, MD 20723, Russell.Fink@jhuapl.edu

² Sherman, Cyber Defense Lab, Dept. of CSEE, University of Maryland, Baltimore County (UMBC), 1000 Hilltop Circle, Baltimore, MD 21250, sherman@umbc.edu, supported in part by DoD H98230-08-1-0334

2 E2E Gaps in Voting System Attributes

While E2E features achieve many desirable election system goals, several gaps remain because of untrustworthy software and poor usability. Table 1 summarizes where TC can improve E2E in each major goal. This analysis motivates applying TC to E2E.

TC can benefit three critical areas: privacy, chain of custody, detecting problems early. Privacy is a major benefit of adding TC to E2E: platform attestation used to control signature keys can allow voting operations only when the system has booted the correct software, mitigating the risks of unauthorized software disclosing private information, such as Scantegrity II ballot codes. Similarly, TPM controls can reduce reliance on trusted chains of custody by ensuring that only the correct platform can access data, and that the data are valid. Verifying correct software operation is crucial to detecting problems early—for example, a trustworthy receipt printer can reveal in the polling place that scanner software has recorded an incorrect selection, allowing the voter to discard her ballot and vote again.

Safer DRE designs can provide good usability, reducing errors in the polling place. In addition to catching undervotes and overvotes prior to casting, studies have shown that voting using electronic systems is generally easier and arguably more preferred than is voting on paper ballots, particularly in long races with many choices (when errors are more likely and difficult to recover from). Accessibility to disabled voters and non-native speakers is a compelling reason for DRE-style interfaces: computerized display and entry apparatus can accommodate differently abled voters through high-contrast displays, audible ballots, puff-and-sip systems for paralyzed voters, and multi-language ballots for non-native speakers.

E2E systems that use touch-screen interfaces can be made safer through *sealed, non-migratable keys* and platform attestation: if the DRE software in Benaloh's [Ben07] voter-initiated auditing were compromised, a coercion mode could be activated by a special sequence of touches applied to the user interface to recognize the voter and bind her identity to her vote. TC can help mitigate this threat: managing the device signature key in hardware and sealing it to the correct platform state would allow the ballot to be signed only when the correct software was running. Additionally, sealing to the TPM prevents theft of the signature key.

Additional benefits include better enforcement of policy and procedures through TPMs; for instance, the *Platform Vote Ballot (PVB)* binding key protocol for DRE voting [Fin09b] signs voter choice and ballot identification data only after a password is revealed on election day. Trustworthy cryptographic logging systems using write-once memory can securely audit interactions in the polling booth. TC complements E2E by preventing malicious software operations, protecting both privacy and transport integrity, thereby enabling computers to provide accessibility to the disabled safely.

TC cannot benefit every aspect of E2E voting. Administration ease, efficiency, cost, and understandability are not aided by TC, and some say TPMs reduce transparency. Significantly, TC requires more complex key management.

3 Conclusions

All voting systems used in large scale elections rely on software for efficiency, usability, and accessibility, but software carries risk (including for privacy) even for software independent verification systems such as E2E. E2E cannot fully satisfy ease of administration, information assurance, and usability alone. TC increases privacy by ensuring the correct software is running. TC helps enable excellent usability and accessibility by making it possible to build trustworthy electronic interfaces. And TC helps voters catch problems in the polling location, making voting safer and better for everyone—at the cost of more complicated engineering design and key management.

Table 1. Trustworthy Computing can enhance E2E systems in varying degrees.

Goal	Attribute	Trustworthy Computing Value Added to E2E
Administration	Auditability	<input checked="" type="checkbox"/>
	Ease of Administration	
	Efficiency	
	Policy Enforcement	<input checked="" type="checkbox"/>
	Total Cost of Ownership	
Assurance	Accuracy	<input checked="" type="checkbox"/> (via electronic interface)
	Authenticity	<input checked="" type="checkbox"/> (ballot authentication)
	Availability	<input checked="" type="checkbox"/>
	Integrity	None – E2E integral feature
	Privacy	<input checked="" type="checkbox"/>
	Public confidence in dispute resolution	<input checked="" type="checkbox"/>
	Repudiated Choice, Non-Repudiated Cast	None – E2E integral feature
	Small Trusted Custody Chain	<input checked="" type="checkbox"/>
Voter Utility	Accessibility	<input checked="" type="checkbox"/> (via electronic interface)
	System Understandability	
	Voter Verifiability	None – E2E integral feature
	Voting Usability	<input checked="" type="checkbox"/> (via electronic interface)
	Identify Problems in Precinct	<input checked="" type="checkbox"/>

Acknowledgments

The authors thank Ron Rivest, Rick Carback, Aleks Essex, and the reviewers for helpful suggestions. Thanks also to Ginny Walker for reviewing this manuscript.

References

- [Ben07] Benaloh, Josh, “Ballot Casting Assurance via Voter-Initiated Poll Station Auditing” in on-line *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop (EVT07)*, USENIX Association (2007). http://www.usenix.org/events/evt07/tech/full_papers/benaloh/benaloh.pdf
- [Chau08] Chaum, David, Aleks Essex, Richard Carback, Stefan Popoveniuc, Jeremy Clark, Peter Ryan, Alan T. Sherman, Ronald Rivest, and Poori Vora, “Scantegrity II: Voter-Verifiable Optical Scan Ballots with Invisible Ink Confirmation Codes” in on-line *Proceedings of USENIX/ACCURATE Electronic Voting Technology Workshop (EVT08)*, USENIX Association (April 2008). http://www.usenix.org/events/evt08/tech/full_papers/chaum/chaum.pdf.
- [Fin09a] Fink, Russell A., Alan T. Sherman, and Richard Carback, “TPM Meets DRE: Reducing the Trust Base for Electronic Voting using Trusted Platform Modules,” *IEEE Transaction on Information, Forensics, and Security* - special issue on voting (April 17, 2009; revised August 7, 2009), to appear.
- [Fin09b] Fink, Russell A., and Alan T. Sherman, “Combining end-to-end voting with trustworthy computing for greater trust, privacy, accessibility and usability,” manuscript (April 17, 2009), 12 pages.