

Toward a Systematic Approach to Voting Process Design and Analysis

Jim Youll

Challenge/Response, LLC
jyoull@alum.mit.edu

David Kong

MIT Media Lab
dkong@mit.edu

December 9, 2004

EXTENDED ABSTRACT

From the confusion over “butterfly ballots” and “hanging chads” in the 2000 elections to fresh troubles with the electronic machines that were supposed to solve these problems in 2004, American elections remain clouded by concern and doubt. Only 40 to 60 percent of voters nationwide even believe their votes were counted in 2004.

In the wake of the difficulties of the past several years, projects such as blackboxvoting.org and the Election Incident Reporting System have sprouted to research, gather, and report system and human failures. Academic and commercial groups including the Caltech-MIT Voting Project, the IEEE Voting Equipment Standards group, and the industry-funded Election Technology Council are also at work developing technical standards and building point-solutions to specific problems with new technologies.

Computerized voting systems are apparently here to stay. But these systems have new failure modes that can lose or mangle more information more untraceably than was ever possible with older equipment. Obvious audits that could catch problems – such as those performed on millions of ATM transactions daily – are not possible in voting systems due to the fundamental, and fundamentally confounding, requirement of absolute voter privacy.

Can a computerized system ever be trusted to count every vote accurately and auditably?

We believe full transparency in the design and operation of voting systems is key to reliable elections, no matter how high- or low-tech the process. We draw parallels between the design ethos of cryptographic systems, and a methodical approach to designing and running voting systems. Cryptographic systems, subjected to continuous reviews of design and implementation, are reliable and trusted. The same could hold for voting systems.

A general means of discussing, designing and evaluating voting systems is needed to reveal vulnerabilities, hidden steps, and points of failure. However, no formal means of rendering voting systems architectures transparent now exists. To fill this need, we propose a “Universal Election Model” (UEM) to capture, organize and visualize a detailed model of the elections process in any locale or technology. Once modeled in the UEM, a system may be analyzed manually or with computer assistance. Some UEM tools will predict ballot spoilage rates for an given process. Others will reveal hidden, unauditible steps. We also propose web and visual tools for modeling and analysis. Through these tools and other materials, the UEM can help voting system buyers and designers, elections officials, and the public better understand the unique risks of their own election processes.

We also describe and will build a “reference implementation” – a best-case example to show how the UEM can drive the design of a fully transparent, fully auditable voting system. The reference implementation will serve as a demonstration tool and platform for experimentation. Finally, we discuss possible educational and public information capabilities of UEM-derived elections systems, and other considerations such as the preferred means of licensing of common election-supporting technologies.

Concerns around fair elections run the gamut from voter registration policies to tricky legal maneuvers. Excluding preparatory and wrap-up work, this project’s specific interest begins when a voter is approved to cast a ballot at a polling place, and ends when a final tally is made and all audits are completed satisfactorily.

This paper and the supporting materials represent a first step toward the creation and public adoption of new means of communicating, analyzing and visualizing voting technologies, processes, and architectures. We invite critique and collaboration. Please address correspondence to the lead author: jyoull@alum.mit.edu

TABLE OF CONTENTS

EXTENDED ABSTRACT	1
INTRODUCTION.....	3
Related Work.....	5
The trouble with machines.....	8
Don't elections officials know better?.....	9
Federal voting systems standards.....	9
State voting systems standards.....	10
Can electronic systems run an assuredly honest election? Can any system?.....	10
Methodology.....	11
Goals.....	18
PROJECT BOUNDARIES.....	12
Specific problems addressed.....	12
TOWARD A SYSTEMATIC APPROACH TO VOTING PROCESS DESIGN AND ANALYSIS.....	13
Vulnerabilities unique to electronic vote collection and counting.....	13
Security, and lessons from other domains and related problems.....	13
Project definition.....	15
1: Universal Election Model (UEM).....	15
2: Analytical and experimental tools.....	23
3: Design guidelines for a successful election.....	24
4: Reference implementation.....	24
5: Educational and public information.....	31
6: Deliverables.....	31
SPREADING THE WORD / CHANGING MINDS.....	32
Appeal to elections officials and the public.....	33
Appeal to vendors.....	33
The cost of a voting machine, and switching costs.....	34
OTHER CONSIDERATIONS, UNRESOLVED ISSUES, OPEN QUESTIONS.....	35
Intellectual property licensing.....	35
Receipts.....	35
Receipt-free post-election audits.....	36
Physical and code security.....	36
Real-time clocks.....	37
Lingering vulnerabilities.....	37
DISCUSSION.....	38
ACKNOWLEDGEMENTS.....	38
APPENDICES.....	39
Mechanical voting machines, images and commentary.....	40
"Found – Artifacts from the future": Wired Magazine voting receipt.....	41
Design sketch: Machine Readable Ballot System for Electronic Vote Counting.....	42
Definitions.....	43