YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 461b: Foundations of Cryptography — *Notes 15 (rev. 1)*
Professor M. J. Fischer — *March 5, 2009*

Lecture Notes 15

37 The Election Problem

Secret ballot elections are an important real-world problem that combines security issues with significant social and political issues. As an introduction to Ron Rivest's 2009 Perlis Lecture on *Security of Voting Systems*, I want to say a little about what the election problem is and why how it differs in fundamental ways from other superficially similar problems such as e-commerce.

Briefly stated, each eligible voter casts a vote for one of a set of candidates for an office. The election system counts the number of votes for each candidate. The candidate with the most votes wins. What could be simpler?

It only becomes hard when we add real-world constraints. We must assume that some voters and election officials are dishonest and are motivated to corrupt the election in favor their preferred candidate, if possible. Already we can see many possible opportunities for corruption. Voters might cast multiple votes. Ineligible voters might cast votes. Voters might not vote for their preferred candidate because of intimidation or for financial gain. Eligible voters might be denied the opportunity to vote. Ballots might be counted incorrectly, and vote totals might be misreported.

The Six Commandments
Democracy is ingrained in the American character and is reflected in its political process from presidential elections down to the most minor of township races. Our passion for fairness and equality has given rise to a set of fundamental requirements for electronic voting systems that are substantially the same from state to state, listed in decreasing order of importance:

I. Thou shalt keep each voter's choices an inviolable secret.

II. Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote [2].

III. Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.

IV. Thou shalt report all votes accurately.

V. Thy voting system shall remain operable throughout each election.

VI. Thou shalt keep an audit trail to detect sins against Commandments II–IV, but thy audit trail shall not violate Commandment I.

[2] Recall that women now constitute a majority of registered voters in the United States.

Figure 37.1: Michael Shamos's axioms for voting systems.

37.1 Shamos's Axioms for Voting Systems

Yale computer science Ph.D. and Duquesne University J.D. Michael Ian Shamos, now at Carnegie-Mellon University, came up with a list of requirements for voting systems that attempt to reflect some of these real-world constraints. The Six Commandments in Figure 37.1 are taken from his paper, *CFP'93 – Electronic Voting – Evaluating the Threat*, 1993, which appears on the Computer Professionals for Social Responsibility (CPSR) web site at `http://www.cpsr.org/prevsite/conferences/cfp93/shamos.html`.

These are a tough set of requirements to meet in practice. Let's see how our existing voting systems work.

1. Votes are kept secret by being dissociated from the voter. With absentee ballots, the dissociation comes only when the outer envelope is opened at the election official's office. With paper ballots, it occurs when the ballot is dropped into the ballot box. With some voting machines, the identity of the voter is never entered into the machine, but this is clearly not true of internet voting, nor would it be true of computerized voting machines that attempted to integrate the voter authentication process with the actual balloting.

2. Voter registration and poll watchers attempt to enforce the principle of one man, one vote. Voter registration is restricted to legally authorized persons. Poll watchers attempt to match voters presenting themselves in person with names on the registration list. The name is crossed off, preventing the same person from voting multiple times. Neither the voter registration nor the voter authentication processes are particularly secure. Registrars often accept a person's signed statement that he or she is eligible to vote without further investigation or documentation. Poll watchers may accept a person's declared identity, or they may require the presentation of some sort if identification card. Little is done to prevent the same person from registering and voting in multiple states, even under their own name, nor is there much to prevent the same person from registering and voting multiple times under different names. Such voter fraud is of course a serious crime, so the threat of punishment and the limited personal gain from successful fraud work together as a strong disincentive to cheat in this way.

3. Tampering with the voting system is discouraged through *transparency*. As much as possible of the election process take place in the open, subject to the scrutiny of representatives of both political parties and other interested groups. Large-scale tampering is hampered by the decentralized nature of the election process. Each election district (in Connecticut) runs its own election and counts its own votes.

   Vote-selling is discouraged by the inability of a voter to provide evidence of how she voted, so a party interested in buying votes cannot know whether or not a voter complied with their wishes. This implies that voting systems must not issue *receipts* that would allow a voter to prove to another how she voted.

4. The tallying of the votes is a two-step process in Connecticut.. The ballots are counted publicly by the precincts. Only the tabulation of the precinct totals is centralized. The latter computation is easily verified through independent computation by news agencies and other interested groups provided they have access to the raw totals from the precincts.

5. Conscientious election officials spend months planning an election to ensure that needed personnel, equipment, and supplies are available throughout election day. Obviously, individual

precincts can and do experience disruptions—power can fail, election workers can be taken suddenly ill, voting machines can malfunction, and so forth, but decentralization again works in favor of the overall election process. A tornado that tears the roof off of one polling place (and yes, that could happen) is unlikely to affect a polling place in the next county or next state.

6. Because of the need to maintain secrecy of the vote, the audit trail is split into two pieces. On the one hand, there are records of who voted (or at least which names on the registration list are marked as having voted). On the other, there are the actual ballots, if paper ballots are being used. The number of ballots cast can be compared with the number of people who voted and should be equal except for the possibility of a voter walking away without depositing the ballot in the ballot box. But the audit trail does not enable one after the fact to verify that the ballots in the ballot box were in fact the ones cast by the voters whose names were crossed off the registration list.

Mechanical voting machines and many direct-recording computerized voting terminals lack the ability to provide a *voter-verified* audit trail. With such machines, the votes are stored internally in the machine until the polls close, at which point election workers read out the totals. Here, there is no way for a voter to know that her vote was counted correctly. Obviously, the total votes cast on a machine can be compared with the number of people who voted on that machine, but there is no way to connect the votes recorded with the votes cast by the voter. With mechanical machines, the linkages between levers and counters are relatively simple and visible. One can have some degree of confidence that the machine is working as intended just through a visual inspection of its innards and some simple testing of its operation.

With computerized voting terminals, all such transparency is lost. One cannot look at a computer and know what is going on inside. Testing is insufficient since computers can easily be programmed to respond normally except when given some kind of coded signal, which might be nothing more than a ballot being cast for a particular unlikely collection of candidates. Such a machine might perform flawlessly during testing, yet corrupt the vote on election day after a malicious voter, in the privacy of the voting booth, cast the coded ballot that triggered the embedded malware. Some confidence might be gained by an examination of the source code, but most voting machine companies consider their code to be proprietary and require through their contracts that it be kept confidential.

37.2 Internet Voting

An interesting question, especially for a cryptography class, is how one might carry out elections completely electronically, on the internet for example. This is not just a hypothetical. The Department of Defense planned to allow troops overseas vote via the internet in the 2004 presidential election. This idea was later scrapped after much protest. (See American Forces Press Service News Article, *Pentagon Decides Against Internet Voting This Year* by Jim Garamone, Feb. 6, 2004.) But such ideas die hard. Bill HB 5903 is now pending in the Connecticut General Assembly to permit electronic submission of absentee ballots for troops stationed overseas.

Internet elections pose serious challenges to almost all of Shamos's commandments. How can an electronic ballot be both private and countable? How can voting be restricted to authorized voters in a way that prevents the tabulating authority from being able to match voters to ballots? How does one prevent tampering with the software used to implement the system, both on the user's computer and also at the central authority? How does one prevent a voter from selling her voter credentials to a third party? How does one prevent a voter from voluntarily letting a third party cast her ballot on her behalf? How can one decentralize an internet voting system so as to obtain some of the robustness that our current decentralized system enjoys? How can one prevent targeted denial-of-service attacks that could disable internet voting for certain groups of voters on election day? What kinds of electronic audit trails are possible, and how can they be verified?

Several election protocols have been devised that attempt to address some of these questions. While none is entirely satisfactory from a practical point of view, they do employ some clever cryptographic ideas that might eventually be useful.