

Electronic Voting: practice and theory

Mark Ryan
University of Birmingham

Computer Security lecture
November 2008

Outline

- 1 The potential
- 2 The current situation
- 3 Desired properties
- 4 An example: FOO'92 protocol
- 5 Conclusions

Electronic voting

Electronic voting has the potential to provide

- **more efficient** elections with **higher voter participation**, **greater accuracy** and **lower costs** compared to manual methods.
- better security than manual methods, such as
 - **vote-privacy** even in presence of corrupt election authorities
 - **voter verification**, i.e. the ability of voters and observers to check the declared outcome against the votes cast.

Governments world over have been trialling e-voting, e.g. USA, UK, Canada, Brasil, the Netherlands and Estonia.

Can also be useful for smaller-scale elections (student guild, shareholder voting, trade union ballots, local government).

Current situation

The potential benefits have turned out to be hard to realise.

In UK

- May 2007 elections included 5 local authorities that piloted a range of electronic voting machines.
- Electoral Commission report concluded that the implementation and security risk was **significant and unacceptable** and recommends that **no further e-voting take place** until a sufficiently secure and transparent system is available.

In USA:

- Diebold controversy since 2003 when code leaked on internet.
 - Kohno/Stubblefield/Rubin/Wallach analysis concluded Diebold system **far below even most minimal security standards**. Voters without insider privileges can cast **unlimited votes** without being detected.

Current situation in USA, continued

- In 2007, Sec. of State for California commissioned “top-to-bottom” review by computer science academics of the four machines certified for use in the state. Result is a catalogue of vulnerabilities, including



- **appalling software engineering practices**, such as hardcoding crypto keys in source code; bypassing OS protection mechanisms, ...
- susceptibility of voting machines to **viruses that propagate from machine to machine**, and that could maliciously cause votes to be recorded incorrectly or miscounted
- **“weakness-in-depth”**, architecturally unsound systems in which even as known flaws are fixed, new ones are discovered.

In response to these reports, she **decertified all four types of voting machine** for regular use in California, on 3 August 2007.

Situation in USA – 2008 election

- Several other states followed California's lead, and decertified electronic voting machines.
- But other states have continued to use touch-screen systems, having invested massively. (E.g., the state of Colorado spent \$41M on electronic voting systems for its 3M voters, on machines that California has now decertified. . .)
- Diebold, one of the main suppliers, tried unsuccessfully to sell their e-voting business. Instead, they rebranded it 'Premier Election Solutions' and revised their forecasts downwards.

Current situation in Estonia

- Estonia is a tiny former Soviet republic (pop. 1.4M), nicknamed “e-Stonia” because of its tech-savvy character.
- Oct. 2005 national election allowed voters to cast ballots on internet. Fewer than 10,000 people (1% of registered voters) participated online.
- Officials hailed the experiment a success. Said no reports of hacking or flaws. System based on linux.
- Voters need special ID smartcard, a \$24 device that reads the card, and a computer with internet access. About 80% of Estonian voters have the cards anyway, also used since 2002 for online banking and tax records.

Internet voting and coercion resistance

The possibility of coercion (e.g. by family members) seems very hard to avoid for internet voting.

In Estonia, the threat is somewhat mitigated:

- Election system allows multiple online votes to be cast by the same person during the days of advance voting, with each vote cancelling the previous one.
- System gives priority to paper ballots; a paper ballot cancels any previous online ballot by the same person.

Where are we?

- 1 The potential
- 2 The current situation
- 3 Desired properties**
- 4 An example: FOO'92 protocol
- 5 Conclusions

Voting system: desired properties

- **Eligibility**: only legitimate voters can vote, and only once (This also implies that the voting authorities cannot insert votes)
- **Fairness**: no early results can be obtained which could influence the remaining voters
- **Privacy**: the fact that a particular voted in a particular way is not revealed to anyone
- **Receipt-freeness**: a voter cannot later prove to a coercer that she voted in a certain way
- **Coercion-resistance**: a voter cannot interactively cooperate with a coercer to prove that she voted in a certain way
- **Individual verifiability**: a voter can verify that her vote was really counted
- **Universal verifiability**: a voter can verify that the published outcome really is the sum of all the votes

... and all this even in the presence of corrupt election authorities!

Are these properties even simultaneously satisfiable?

Contradiction?

- **Eligibility**: only legitimate voters can vote, and only once
- **Effectiveness**: the number of votes for each candidate is published after the election
- **Privacy**: the fact that a particular voted in a particular way is not revealed to anyone (*not even the election authorities*)

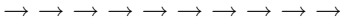
Contradiction?

- **Receipt-freeness**: a voter cannot later prove to a coercer that she voted in a certain way
- **Individual verifiability**: a voter can verify that her vote was really counted
- **Individual verifiability (stronger)**: . . . , and if her vote wasn't counted, she can prove that.

How could it be secure?



Security by trusted client software



- trusted by user
- does not need to be trusted by authorities or other voters

- not trusted by user
- doesn't need to be trusted by anyone

Where are we?

- 1 The potential
- 2 The current situation
- 3 Desired properties
- 4 An example: FOO'92 protocol**
- 5 Conclusions

First, some cryptography

Blind signatures

- Normally, when Alice signs a message M , creating $\text{Sign}_{SK_A}(M)$, she knows what the message M is.
- In a **blind signature**, Bob can ask her to sign a **blinded version** of the message, $\text{blind}_b(M)$.
- After she signs it, he can **unblind it**.

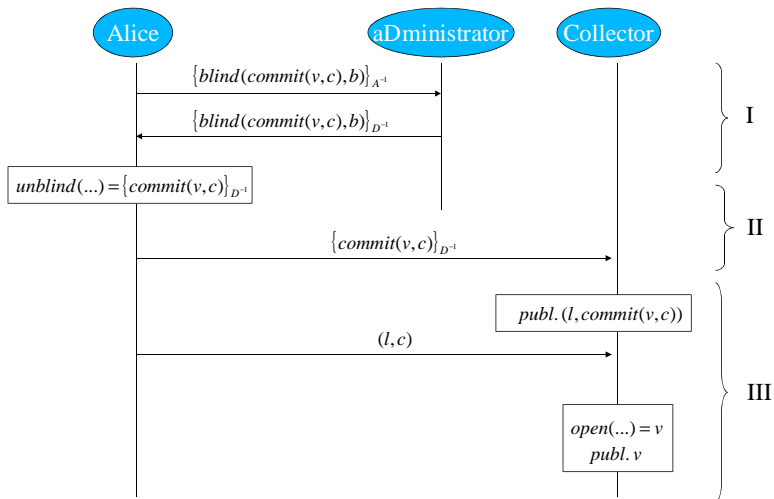
$$\text{unblind}_b(\text{Sign}_{SK_A}(\text{blind}_b(M))) = \text{Sign}_{SK_A}(M)$$

Commitments

- Alice can send Bob a **commitment** $\text{commit}_c(M)$ to a message M .
- Later, she can reveal c and M , and Bob can verify that it is indeed the correct M that she committed to.
- Alice cannot lie, e.g., cannot find some other c' and M' that have the same commitment $\text{commit}_{c'}(M')$.

FOO 92 protocol

[FujiokaOkamotoOhta92]



FOO 92 properties

Let us consider for each one whether FOO has it or not:

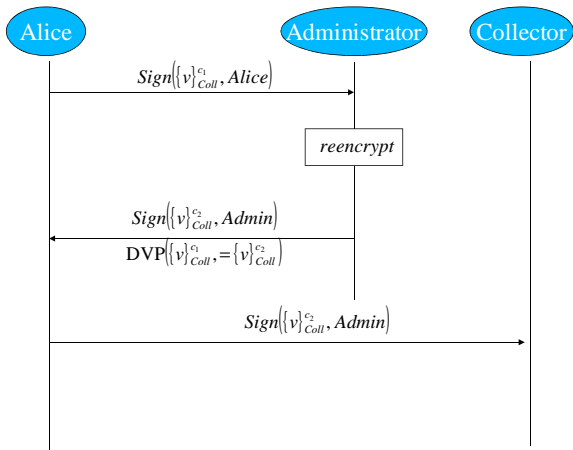
- Eligibility
- Fairness
- Privacy
- Receipt-freeness
- Coercion-resistance
- Individual verifiability
- Universal verifiability

4 out of 7. . . . not too bad!

FOO usability in a real election: an exercise for the reader.

LBDKYY'03 protocol

[LeeBoydDawsonKimYangYoo]



Conclusions

- Electronic voting is coming, whether we like it or not.
- Sadly, the current systems are woefully inadequate.
 - in the USA and UK, they don't manage to satisfy basic security properties, like resistance to virus attacks and to tampering.
 - They don't even try to satisfy stronger properties, like privacy guarantees against corrupt election officials, universal and individual verifiability.
- There are many “academic” protocols which have much better properties, although some of the earlier ones have usability issues.