Prospects for a Robust Electronic Voting Scheme for the UK

Tim Storer and Ishbel Duncan

University of St Andrews

Overview

- Introduction to electronic voting.
- The UK's Electoral Context.
- Pollsterless remote electronic voting schemes.
- The mCESG Scheme.
- Adapting the mCESG scheme.
- Future work

Elections a Critical Infrastructure?

Poll terror attack risk 'higher'. BBC News, 18th April 2005.

"*Britain faces its greatest risk of terrorist attack yet amid fears that groups may target the general election, according to an annual risk assessment.*"

Jimmy Burns and Ben Hall. **Britain fears al-Qaeda terrorist attack during election**. Financial Times, 24th February 2005.

"*The UK remains vulnerable to the real and serious threat of terrorism by al-Qaeda, according to research by leading academics on the country's preparedness for future attacks.*"

Election and wedding make Britain 'prime terror target'. Daily Mail, 24th February 2005.

"*Britain's most senior police officer issued a stark warning today about the risk of a terrorist attack in the run-up to the General Election.*"

Richard Norton-Taylor. **Threat of terror attack on London higher, says report**. The Guardian, 19th April 2005.

"*The likelihood of a terrorist attack on London has increased because of the impending election and Britain's support of the war on Iraq, according to a private risk assessment published today.*"

Some Terminology

Often used interchangably, but to disambiguate:

Voting system – the set of procedures and technologies used to conduct an election.

Election – an execution of a voting system.

Vote – the expression of a voter's preference.

Electoral system – the description of a legal vote and the algorithm for aggregating votes into results.

Voter – an agent within the voting system eligible to cast a vote.

Ballot – the instantiation of a vote, paper ballot for example.

Voting scheme – theoretical design expressing properties for a a voting system.

Voting technology – the implementation of aspects of a voting scheme.

Why e-voting?

Given the challenges involved, why use e-voting?

- For the US, potential for greater accuracy in:
  - Recording of voter intentions.
  - Aggregation of votes.
- In the UK, remote electronic voting perceived as a means for increasing convenience (and hopefully turnout).
- Other reasons:
  - A useful target topic for development of dependable technologies.
  - A 'modern' way to run elections.

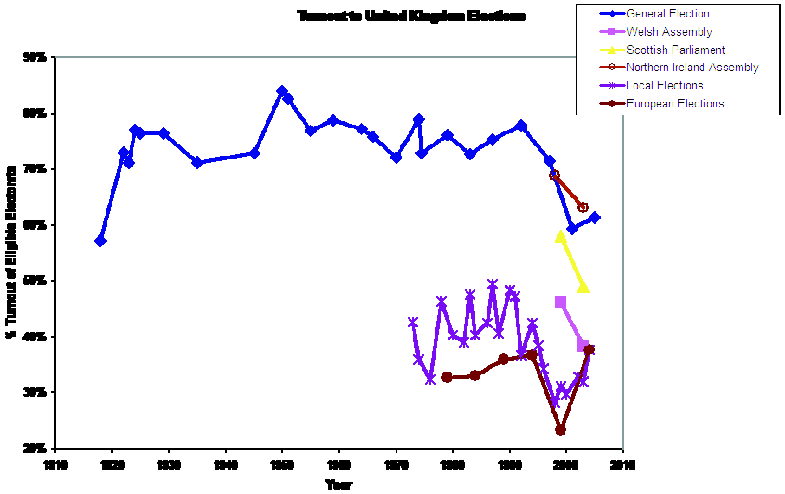
Different contexts have different motivations for changing their voting system.

Threats to e-voting

Numerous, varied and context dependent:

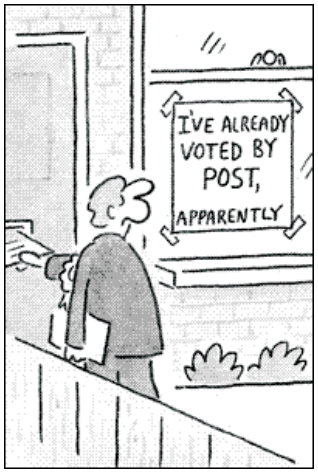
- Loss of vote records result of
  - System failure
  - Corrupt insiders
- Malicious candidates
  - Vote buying
  - Voter coercion
- Denial of service
  - Direct attacks on polling stations.
  - Disruption of power supplies.
  - Disruption of communication networks.
  - Sabotage of voting system.
- Dishonest voters – false claims of fraud.

Trends in Turnout (UK)



Not Just e-voting...

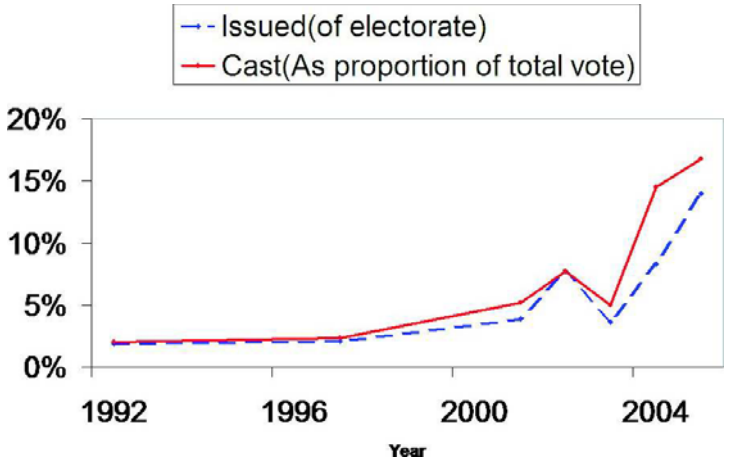
Postal voting on demand caused problems in Birmingham's 2004 Local elections:



Robust Electronic Voting Systems

- Exhibit desired properties despite the presence of faults/attacks:
  - Core properties must be preserved regardless.
  - Some degradation of service may be acceptable.
- This definition is context dependent – required properties in other categories vary.
- Fulfillment of robustness requirements may be achieved through a variety of technological and/or procedural solutions.

Trends in Postal Voting (UK)



The UK Electoral Context

The design of voting schemes is informed by their target context:

- UK Elections are governed by various Acts of Parliament, but primarily the RPA 1983.
- Variety of electoral systems employed – FPTP, AM and STV.
- Weak identification and authentication mechanisms.
  - Registration is by household.
  - No identification documents required at a polling station.
- Vote tracing mechanism permits election recovery without substantially violated privacy.

Requirements

Again, context dependent but with recurring themes:

- Secrecy
  - Voting privacy (remote/supervised)
  - Voter anonymity
- Integrity of result
  - Authentication of legitimate voters
  - Accurate recording of individual votes
  - Accurate aggregation of results
- Usability – # of interactions, interface capabilities.
- User Acceptablity – understandability, familiarity.
- Flexibility – one scheme/system for several contexts?

Pollsterless Electronic Voting

- First noted by Malkhi, pollsterless schemes permit vote casting directly by the voter without a software artifact (a pollster) acting on the voter's behalf.
- Pollsterless schemes have two advantages:
  - A wider range of electronic devices can be used for vote casting and verification.
    - Lowers the cost of participation for voters.
    - A more flexibile range of voting devices improves usability and accessability.
  - Verification of vote collection and tabulation may be performed directly – a voter doesn't need to trust the pollster to intrepret messages on their behalf.

Electronic Voting Approaches

- SERVE (US DoD)
- Homomorphic encryption (Benaloh)
- Blind signature schemes (Fujioka)
- Cryptographic Counters
- FREE e-Democracy (Kitcat)
- SENSUS (Cranor)
- REVS + variants (Joaquim)
- RIES
- Cybervote Project (EU)
- Hybrid DRE/Paper ballot systems
  - Paper audit trails.
  - 'Mercuri' method.
- 'Hybrid' schemes utilising mix–nets:
  - Multiple receipts (Shubina)
  - VoteHere (Neff)
  - Visual cryptography (Chaum).
  - Prêt á Voter - (Schneider/Ryan/Bryans)
- ...

The mCESG Scheme

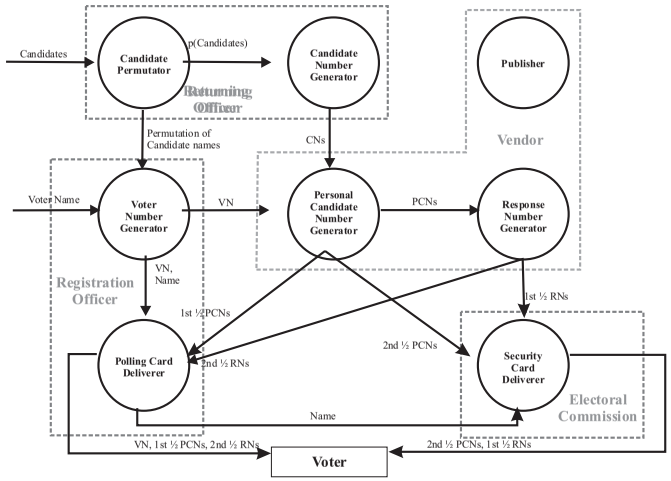
- The CESG scheme was proposed by the commerical arm of GCHQ.
- The mCESG scheme improves on the CESG scheme by:
  - Providing vote verification without increasing potential for coercion/vote buying.
  - Distributes the election authority into autonomous domain to provide better protection of voter privacy.
- Retains the pollsterless feature of the CESG scheme for vote casting.

Common Countermeasures

- Distribute trust across autonomous domains.
- Maintain failure detection and recovery mechanisms.
  - Detection by officials, candidates or voters.
  - Non–trivial in presence of secrecy requirements.
- De–centralised vote collection points (polling stations).
  - Identification of bottlenecks in voting schemes is an emerging topic.
- Provide mechanisms for voter and/or universal verifiability.

Credential Generation

The domains of the election authority co-operate to generate credentials.



Scheme Overview

The mCESG electronic voting scheme has four phases:

1. Voter registration.
2. Distributed credential generation.
3. Voting.
4. Tallying.

Phases two and three may occur in parallel, i.e. voting credentials may be requested during the voting period.

Casting a Vote

- Send a combination of `<VID>` and `<PCN>` to the election authority on any available communication device.
- To vote for Mrs Thatcher, send:

$$\underbrace{4547129037384571}_{\text{VN}}\ \underbrace{1642}_{\text{PCN}}$$

  In an SMS message to the election authority.
- A generic reply is received:

```
''Thankyou for voting --
you have not been charged for
your text message.''
```


Voting Credentials

- Consists of a *polling card* and a *security card*, delivered seperately to the voter on secure stationary.

Voter Name: Alice JONES
Voter Number: 4547 1290 3738 4571

Candidates	Personal Candidate Numbers		Response Numbers	
M. Thatcher	16	42	712	583
N. Chamberlain	67	24	835	572
C. Atlee	60	12	932	701

SECURITY CARD

POLLING CARD

- Credentials are generated across a distributed election authority to resist ballot box stuffing.

The Bulletin Board

Before: **After:**

Response Numbers	Candidate
642312	N. Chamberlain(Dinner Party)
712583	M. Thatcher(Tea Party)
076894	N. Chamberlain(Dinner Party)
636639	M. Thatcher(Tea Party)
796793	N. Chamberlain(Dinner Party)
…	…

Verifying a Vote

Before the close of poll a voter can confirm their vote was collected:

- Votes collected by the election authority are translated into their corresponding response numbers (RIDs):
  <VN><PCN> → <RID>
- For Alice's vote:
  4547129037384571164 2 → 712583
- The response numbers are then published on a secure, universally accessible bulletin board.
- Voters access the bulletin board to confirm that the correct response number for their choice (on the voting credentials) has been recorded.

Receipt Freeness

mCESG provides voters with a receipt for their vote which corrupt candidates may demand off them.

- Desirable to make mCESG receipt–free.
- Prevent vote-selling after the fact.
- Harder to prevent credential selling prior to voting.
  - A phenomenon of all remote voting systems.
- for mCESG vote as normal, but change verification mechanism.
  - Provides receipt–freeness for most voters.

Verifying a Vote 2

After the close of poll, a voter can confirm that their vote was correctly counted.

- The name of the candidate for each response number published is also published on the bulletin board.
- For Alice's Vote:
  712583 | M. Thatcher
- Alice can request the candidate, but not the response number be changed at this stage.
- Since all votes are published for verification, vote counting is an open process, performable by any external observer.

Open Research Questions(1)

- Even with recovery mechanisms, desirable to build an implementation that:
  - "almost never" has to use recovery mechanisms
  - doesn't threaten security properties
  - limits the potential for attacks on bottlenecks
- Is N-versioning a potential mechanism for providing robustness?
- How should e-voting schemes be measured against existing technologies?
- Do elections have an acceptable failure rate?

Revised Polling Card

Separate the response number between acknowledging vote and choice:

Voter Name: Alice JONES
Voter Number: 4547 1290 3738 4571
Personal Response Number: 7125

Candidates	Personal Candidate Numbers		Response Numbers	
M. Thatcher	16	42	8	3
N. Chamberlain	67	24	7	2
C. Atlee	60	12	0	1

SECURITY CARD

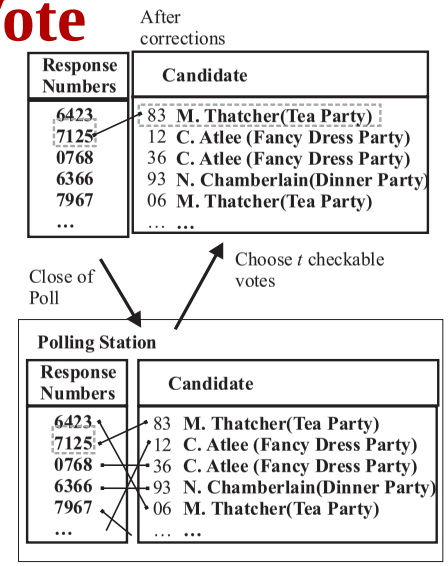
POLLING CARD

Open Research Questions(2)

- Distribution of voting authorities:
  - Greater efficiency through centralisation vs distribution for robustness.
  - How should policy on vote aggregates reporting be enforced?
- What are the implications (for the system and the voter) of conducting a scrutiny?
- What (un-anticipated attacks) is the scheme vulnerable to?

Verifying a Vote

- Voter response numbers are published as votes are collected.
- At the close of poll, the election authority commits to votes.
- Candidates choose t response numbers to be checked by voters.
- t voters confirm correct candidate for response number.



Summary

- Electronic voting represents an ideal target topic for the development of robust technologies.
- Potential for greater accuracy and convenience from electronic voting schemes/systems, particularly for complex electoral contexts.
- Pollsterless remote electronic voting schemes offer greater simplicity and flexibility for the voter.
- The mCESG scheme is adaptable to different electoral systems and requirements.
- Future work will focus on:
  - the usability of the scheme and its variations.
  - improving the receipt–free variation using other committment techniques.

Open Research Questions(3)

HCI, procedural and acceptance issues:

- Is the vote communication mechanism sufficiently usable?
- Can the scheme be adapted for ordinal electoral systems?
- Management of multiple votes over multiple channels (which one counts?).
- What proportion of vote checkers is needed to resist insider attacks?
- How should the scheme be implemented to recover from catastrophic failure?
- For what period prior to polling day and before close of poll should a system be available?
- What criteria should be used to measure user acceptance (voters, candidates, officials)

Future Work

- Dependable implementation of architecture
  - desirable to not have to implement recovery mechanisms.
  - mustn't violate security properties.
- l-round verifiability check for more convenient receipt–free verifiability.
- Live usability and user acceptance testing.
  - Early experiments indicate voters still mistrust even simple electronic voting schemes.
- Stronger proofs of correctness.
- Secure bulletin board design.
- Employ candidates in credential generation, e.g. multi–party computation.