Some Problems with End-to-End Voting

Douglas W. Jones
Department of Computer Science
University of Iowa
Iowa City, Iowa
jones@cs.uiowa.edu

supported, in part, by NSF
Grant CNS-05243

Presented NIST Workshop on End-to-End Voting Systems, Oct. 14, 2009, Washington DC.

The Secret Ballot Problem

How secret are end-to-end ballots?

- Not all are receipt-free:
  - Scantegrity II ballots retain serial numbers
  - Prêt á Voter serial numbers clipped from ballot
- End-to-end property requires that:
  - Voter may retain link to encrypted ballot
  - State retain keys to decrypt ballot
- Ballot secrecy is conditional, not absolute

The Ballot Act, 1872, Britain

2. In the case of a poll at an election the votes shall be given by ballot. The ballot of each voter shall consist of a paper (in this Act called a ballot paper) showing the names and description of the candidates. Each ballot paper shall have a number printed on the back, and shall have attached a counterfoil with the same number printed on the face. At the time of voting, the ballot paper shall be marked on both sides with an official mark, and delivered to the voter within the polling station, and the number of such voter on the register of voters shall be marked on the counterfoil, and the voter having secretly marked his vote on the paper, and folded it up so as to conceal his vote, shall place it in a closed box in the presence of the officer pre-

Types of Ballot Secrecy

- Conditional secrecy: Ballot is secret if both
  - Voter does not disclose ballot ID
  - State does not unseal ballot ID data
    - Ballot act of 1872 is a perfect example
- Absolute secrecy:

"... ballots without any distinguishing mark or symbol"

- Virginia consititution of 1902

"... secure to every elector absolute secrecy in preparing and depositing his ballot"

- Washington constitution of 1889

End-to-end Voting

- OK under British model
  - Cryptography improves the British model
- Problematic under absolute model
- In theory, voter and ballot can be linked
- The voter and the key custodians can cooperate
- Legal definitions of ballot secrecy are slippery
  - Wording does not admit to middle ground
- End-to-end systems used under absolute laws force us down a slippery slope.

The Slippery Slope at Work

Washington constitution:

- As worded, places obligation on the state
  - State must secure secrecy for every voter
- As interpreted, gives voters a right
  - Voter may waive right to secrecy
- The consequence
  - Washington now uses universal postal voting
  - There is a general consensus that the secrecy properties of postal ballots are very weak.

International Law

The Charter of Paris, 1990:

> "... ensure that votes are cast by secret ballot or by equivalent free voting procedure and that they are counted and reported honestly with the official results made public."

OSCE ODIHR draft interpretation, 2008:

- Requires sufficient transparency that observers can determine degree of secrecy of ballot and honesty of counting.

This might be a model for both developers and legislators

Transparency Failures

RIES, the Rijnland Internet Election System.

- Used in the Netherlands for expats, 2006
- ~20,000 votes
- End-to-end publically verifiable, not receipt free

Integrity depends on:

- PRNG keys used to generate codebook
- Keys should be destroyed immediately

Problems with RIES

Timing

- Codebook generated at start of election cycle
- This is before anyone is organized to observe

Security constraints

- Proof of destruction of information is difficult
- Best done in presence of observers

Bureaucrats

- If it's critical, do it behind locked doors
- Always keep backups