April 25, 2005 -- Lecture 37

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Voting

Voting: Trivial Except for Security

Voting is simple:

You go to the polls, then they count your votes and announce the winner!

Voting is a distributed process

Many precincts, situated in
Many jurisdictions (counties)

The central security problem:

Every participant has motive to cheat
Voters, administrators and observers
There are no neutral third parties!

The Australian Secret Ballot

VICTORIA, AUSTRALIA, 1858

Print ballots at government expense

All qualified candidates are listed for each race on ballot

A blank ballot issued to each voter

at the polling place under supervision
voter votes ballot and places in box

At close of polls

all ballots in box counted

Entire procedure open to public scrutiny

Attacks on the Australian Ballot

Ballot box stuffing

At opening of polls, show empty box.

Voter casting multiple ballots in one session

Strict control over blank ballots.

Hand ballot to official to put in box.

Official adding ballots during election

Box in public view at all times.

Chain Voting

Suggest that voter

Take pre-voted ballot to polling place.
Get blank ballot from polling place.
Offer to pay on receipt of blank.

Crook

Needs one blank ballot at start of day.
Can vote each new blank ballot.

One unaccounted for ballot
translates to many bought votes.

Defense against chain voting

Prevention measure:

Strict accounting for all blank ballots.
from printing press to polling place.

Interfere with process:

Serial number on ballot.
Record serial numbers when ballot issued.
Match ballot number when ballot voted.
Enforce time limit between issue and vote.

Ballot numbers could violate privacy

Ballot Secrecy

Prevents

Coercion of voters to vote as approved

Requires

- nobody can observe how you voted
- you cannot disclose your vote

Two models:

British: State forbidden to examine who voted which ballot except under court order.

American: All ballots anonymous, so that corrupt government cannot cheat.

Put ballot numbers on tear-off stubs

Vote Counting:

Two models:

- *Precinct count - count votes at precinct then report totals*
  - Distributed counting hard to oversee
  - Count then transport improves security
- *Central count - transport votes to counting center, then count*
  - Central counting easy to supervise
  - Transport prior to count is vulnerable

Issues, in either case

- *Secure transportation*
- *Honest counting*

Secure transport:

Chain of custody:

Ballots are evidence in a potential case
Therefore, document who had them when

Transport by:

Those with training in rules of evidence

Law enforcement personnel
What if the county sheriff is a crook?

Two election workers of opposing parties

Fails if there are many parties
with shifting coalitions.

Ballot counting

It's not the voting that's democracy, it's the counting.

(Tom Stoppard, British playwright, 1972)

You won the election, but I won the count.

(Anastasio Somoza, Dictator, 1977)

Count

in public, in plain view of observers
ballots, not votes

Tally teams

made of members of opposing parties

Sort ballots

into those where team members agree
(pile for each candidate, pile for no vote)
and those where team members disagree

Resolution of disagreements must be subject to closest scrutiny

A Ballot Secrecy Problem

Suppose a voter signs his ballot

This is disclosure to tally team

Could enable pay-off to voter for vote

To prevent this

Disqualify ballot with "distinguishing marks"

Must prevent tally team from adding marks

Forbid pencils to tally teams.

Require manicure or white gloves.

What is a distinguishing mark?

Use write-in vote as signature.

Use eccentric vote pattern as signature.

Retain all evidence in case of contest

All evidence:

Voted ballots
Documentation of chain of custody
Documentation of resolution of conflicts
Counts of voters signing in to polls
Counts of ballots issued

Federal law: 22 month retention

All records should be public

Except where disclosure can be shown to threaten election security (never require disclosure of passwords)