Mar 25, 2005 -- Lecture 24

22C:169
Computer Security

Douglas W. Jones

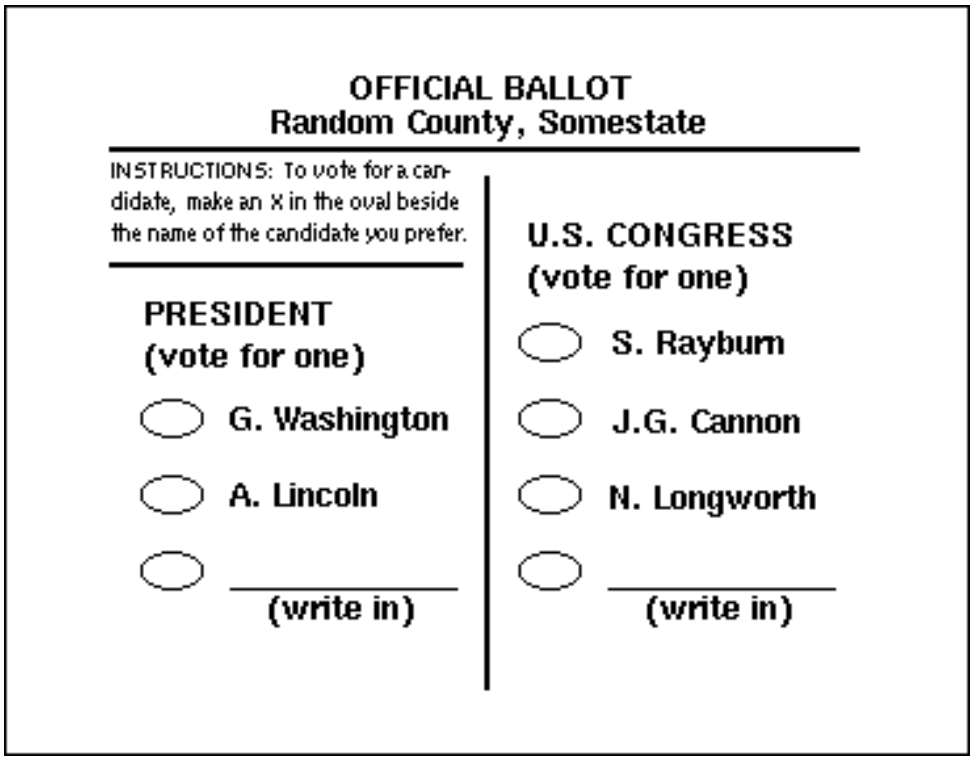
Department of Computer Science

Conflicting Specs

Example of Conflicting Requirements

Elections

Database contains all ballots cast



OFFICIAL BALLOT
Random County, Somestate

INSTRUCTIONS: To vote for a candidate, make an X in the oval beside the name of the candidate you prefer.

PRESIDENT
(vote for one)

- G. Washington
- A. Lincoln
- _____ (write in)

U.S. CONGRESS
(vote for one)

- S. Rayburn
- J.G. Cannon
- N. Longworth
- _____ (write in)

Typical Election Requirements

Integrity
: Ballots may not be lost or altered

Privacy
: Nobody may find out how you voted

Secrecy
: You may lie about your vote

Auditability
: It is possible to show that the above constraints were met

Openness
: All election records are public

Security threats

Ballot box stuffing

An election official adds extra ballots

Defense: public demonstration of empty box at start, public scrutiny to prevent manipulation.

Double voting by a voter

A voter tries to vote multiple ballots

Defense: mechanism or human procedure for casting ballots.

Security Threats II

Vote buying or coercion

rewarding voters for voting correctly

punishing voters for voting incorrectly

Defense: Private and secret ballot,
(this is easier to say than to do).

Denial of service

skew results by slowing voting

where demographics are "wrong"

Defense: Procedural safeguards.
(this is easier to say than to do).

Security Threats III

Destruction of ballots

target precincts based on demographics or target "bad" ballots during counting

Defense: Publish ballots as soon as possible.

Substitution of counterfeit ballots

man in the middle attack on data sent from polling place to counting center

Defense: Immediate publication, redundant transmission, document chain of custody.

Integrity, auditability and openness

These are compatible

- *Keep a transaction log*
- *Who cast what ballot when*
- *Publish log and ballots*

Observers can easily determine

- *Who voted when*
- *Compare this with log*
- *Compare log with ballot database*

Privacy and Secrecy

These are compatible

keep no transaction log
randomize ballots in ballot box
publish ballots only after all votes cast

We have a conflict here
Building a voting system that
meets these conflicting demands
is extraordinarily difficult