CS-438 Decentralized Systems Engineering

Fall 2022

Week 14

Electronic voting

Process - phases

Prepare ballots
- format
- identify voters
- 1 ballot → each

Cast ballots
- ensure accuracy, privacy

Count ballots
- accurate count (1 voter 1 vote)
- verifiability → trust

Requirements

- Authentication - only eligible voters vote
- Equality/fairness - 1 voter 1 vote
- Integrity - mark, cast, counting
- Privacy of choices
- Transparency → E2E verifiability

Electronic voting approaches

In-person voting

- Computer assists in ballot marking, casting
  Ballot Marking Devices (BMD)
  - validates user choices
  - assistive techs (screen reading)
  - counting efficiency
  - convenience
- 2 varieties:
  - all-digital (- digital ballots)
  - paper trail (STAR vote) - paper ballots

Remote voting (E-voting, I-voting)

- Switzerland, Estonia, ...
- mark ballots electronically on own devices
  - transmit over Internet
  - hope (verify) counted correctly
  - no paper trail

Remote voting phases

Registration - decide on voter roster
Open election
Ballot casting - Encryption, transmission
Close election
Shuffling - randomize order of encrypted ballots
Counting - Decryption of ballots (or tallies)

End-to-end verifiability

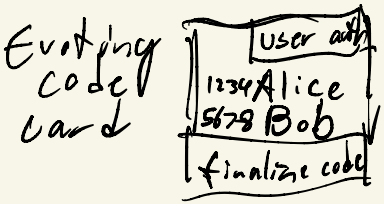
Verifiability properties:

- Cast-as-intended: voter's intent $\xrightarrow{V}$ encrypted, transmitted ballot
- Recorded-as-cast: encrypted ballots $\xrightarrow{V}$ ledger of cast ballots
  "public bulletin board" PBB or ledger/blockchain
- Counted-as-recorded: all recorded encrypted ballots $\xrightarrow{V}$ shuffle, decrypt, count

Cast-as-intended — challenges

- Net connectivity (availability) — Swiss E-voting: can fall back to postal or in-person
- Ballot manipulation in network (MITM) — strong user authentication
- Compromised voter device

"code voting"



Voter:
1. sign in w/ device
2. enter choices
3. finalize, enters "finalize" code
4. server → device & user codes of user's choices
5. confirm, transmit

Counted as-recorded

- Shuffle-and-decrypt
  - Classic mix-nets (Chaum-style Mixminion)

cascade: ballots → O → Ó → ... O → decrypted ballots

MIX 1 ↑ MIX 2

verifying

  - Cut-and-choose (Scantegrity)
  - Cryptographic verifiable shuffles

Neff, ... - ZKP

- Coercion-resistance?