Threat models

Basics of threat modelling

- Threat actors
- Adversaries
- Capabilities of adversaries
- Trust vs verifiability
- Clear articulation of all trust points

Case study: Authentication and KYC

Trust model of old-fashioned identity cards

- Presenter trusted?
- Verifier trusted?
- KYC based on identity documents?

Trust model of old-fashioned identity cards

- Presenter trusted?
- Verifier trusted?
- KYC based on identity documents?
    - Possibilities of repurposing?
- Vacuous?

Trust model of smart cards with chips

- Content trustworthy?
    - Under what conditions?
- Presenter?
- Verifier?
- Verifier machine?

Trust model of Aadhaar Based Biometric Authentication

- No trust requirement on presenter?
- What about verifier?

Trust model of Aadhaar Based Biometric Authentication

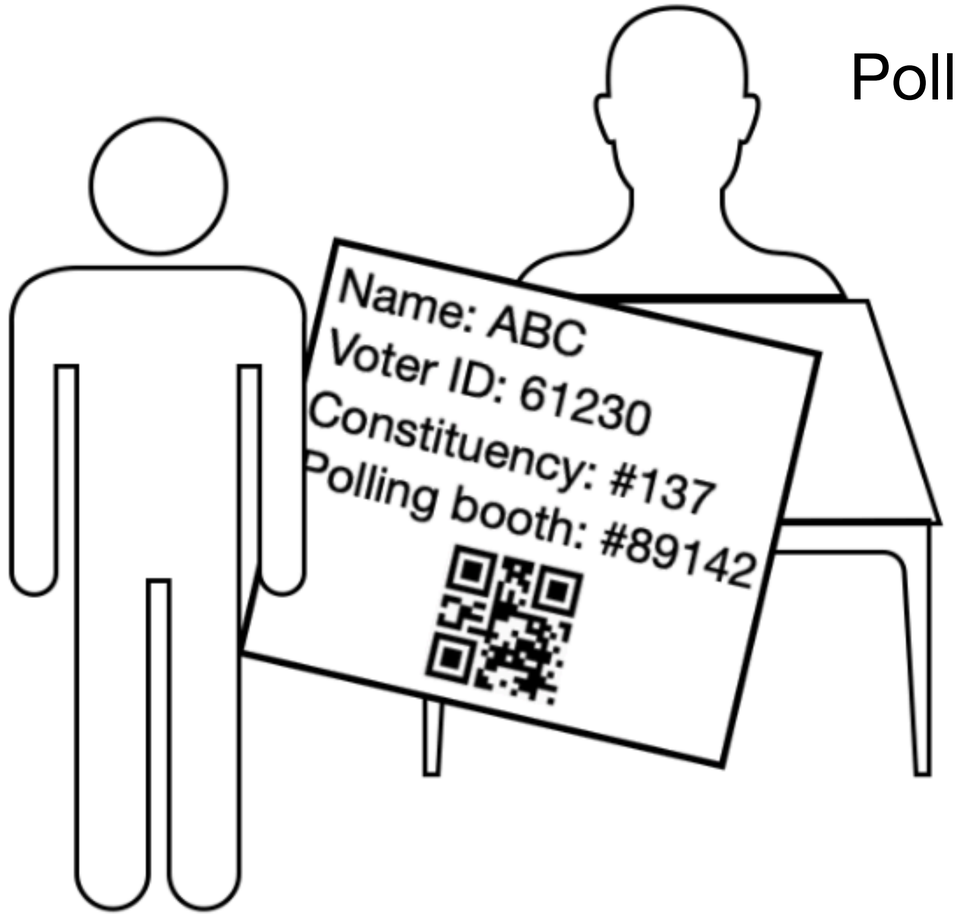
- No trust requirement on presenter?
- What about verifier?
    - Assume cannot control backend
    - False authorisation and/or accounting?
    - Store and replay?
- What if authentication outcome is routed through the verifier?

Trust models of other authentication methods?

- Passwords
- Ssh authentication (Diffie-Helman key exchange)
- Kerberos authentication

Case study: elections

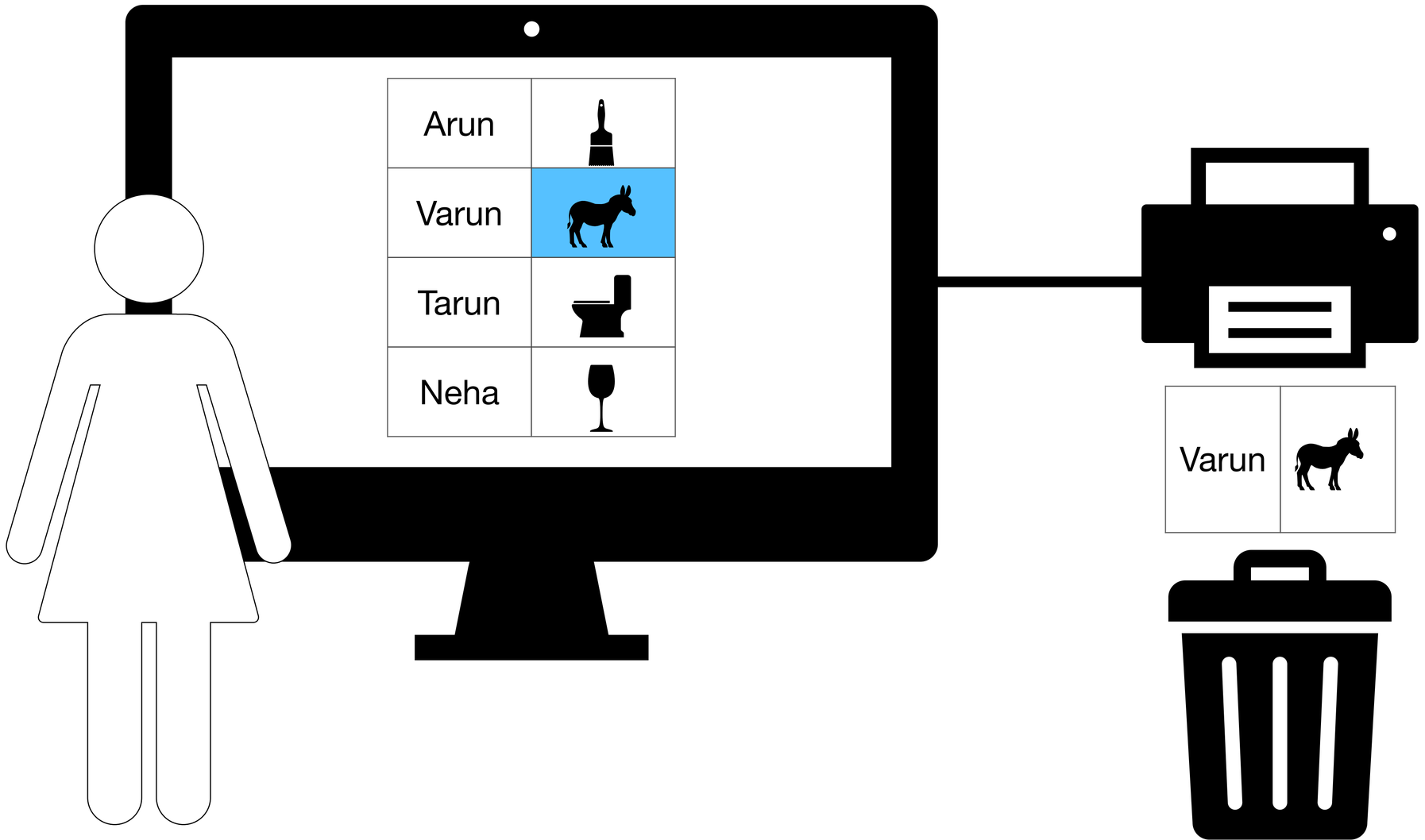
Identity and eligibility verification



Polling officer

Also polling agents

EVM + VVPAT



Security threat analysis

Threat model

- Adversary can corrupt and control
    - An arbitrary set of polling officials
    - An arbitrary set of voters
    - Voting equipment

Voting requirements

- Correctness
    - Cast as intended
    - Recorded as cast
    - Counted as recorded
    - Only eligible voters and only 1 vote per eligible voters
    - Non-repudiation and dispute resolution
- Secrecy
    - Receipt free (voter should not be able to prove who she voted for)

Formal definitions

Threat model for verifiability

The adversary $A_{verifiability}$ is a polynomially bounded adversary who may try to alter the outcome of the election. It

1. can corrupt the EA, the POs, the voting machines, or any other authorities;
2. can alter or delete cast votes during polling, during the collection and counting processes, or while publishing on public bulletin boards;
3. can introduce fake votes in the system, i.e., those not certified by polling officers;

Verifiablity

Universal verifiability: A voting system is universally verifiable if anyone in the public can verify using publicly posted data that

1. each vote is recorded-as-cast and counted-as-recorded
2. all recorded votes are cast by eligible voters
3. any eligible voter has cast at most one vote

Individual verifiability: A voting system is individually verifiable if any voter can obtain a sound proof that their vote is recorded-as-intended in the final tally

Verifiability: A voting system is verifiable if Universal verifiability and Individual verifiability hold in the presence of $A_{verifiability}$

Threat model for secrecy and coercion resistance

The adversary $A_{secrecy}$ is a polynomially bounded adversary who may try to learn others' votes, or coerce them to vote in a certain way, or be a voter itself and try to prove to others how it voted. It

1. can observe all voter receipts, VVPRs (during counting) and public outputs posted on bulletin boards;
2. can participate as a bare-handed voter;
3. can interact with other voters before and after the voting process but not during;
4. can control POs and election authorities;
5. can corrupt voting machines to reveal votes or other secrets;
6. *cannot* observe secrets of to-be-used paper ballots between printing to their usage without leaving a trace of tampering;

Secrecy and coercion resistance

Individual vote secrecy: A voting system protects individual vote secrecy if given a (possibly malicious) voter's receipt and publicly posted data, no information can be derived about how the voter voted. That is, a voter cannot prove to anybody how she voted.

Community vote secrecy: A voting system protects community vote secrecy if given voters' receipts and publicly posted data, an adversary cannot determine how voters assigned to a given polling booth voted.

Secrecy preserving and coercion resistant: A voting system is secrecy preserving and coercion resistant if the above two properties hold even in the presence of $A_{secrecy}$

EVM+VVPAT system

- Verifiable?
- Secrecy preserving and coercion resistant?

EVM+VVPAT system

- Verifiable?
- Secrecy preserving and coercion resistant?
- **Software independent**: A protocol is software independent if an undetected change in the software cannot cause an undetectable change in the (election) outcome
- Software independence a necessary condition for both verifiability and secrecy?