Discussion of Indirect Voter Association

This document highlights the cybersecurity working group discussion around the indirect voter associations (IVAs) by a voting system. IVAs are noted as an open area due to concerns around ballot secrecy. This document will list the potential use cases for IVAs, identify the threat concerns, and discuss current VVSG 2.0 related principles, guidelines, and/or requirements.

Overview

Decision Points

- Are Indirect voter associations necessary for certain voting systems?

Use Cases

Future Uses

- E2E verifiable paperless system handling conditional ballots (e.g., provisional ballots)

The following sections describe the concerns with using or excluding IVAs in the voting system and suggested mitigations to those concerns. The concerns and mitigations do not represent a consensus opinion, but rather an aggregation of what was discussed by the cybersecurity working group.

Primary Concerns with Using Indirect Voter Associations

Concern A.  Principle 10: Ballot Secrecy, Guideline 10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections. If a voter cast’s their ballot using an E2E verifiable paperless system, the voting system will need a way to process conditional ballots, such as provisional ballots. This would require to the voting system to store an IVA to remove a voter’s ballot if they are found ineligible.

Suggested Mitigations:
Indirect Voter Association Analysis

This section steps through a list of indirect voter association uses cases that are relevant to scope of the VVSG requirements. Each use case is followed by concerns, suggested mitigations and related requirements.

---

E2E Verifiable Paperless System Handling Conditional Ballots

Conditional ballots are completed and submitted by a voter for review of voter eligibility. Ballots that are completed and submitted through an electronic system (e.g., E2E paperless system), may require an indirect identifier to locate and remove the ballot if a voter is found ineligible. There are three common scenarios for conditional ballots:

1. **Provisionals** - If a voter is unable to confirm their identity at the polling place, the voter is allowed to complete and submit a ballot for eligibility review.
2. **Absentee/Military Voting** – Ballots may be submitted in advance due to a voter’s schedule or other unavoidable circumstances.
3. **Change of Eligibility** – A ballot must be removed from the official count due to a change in a voter’s eligibility status (e.g., death or relocation).

**Concerns**

**Ballot Secrecy Violation**

If the indirect voter associations are stored on the voting system. Due to their nature, the indirect voter associations may allow an attacker to extract the indirect voter associations and use them to correlate a voter with their ballot selections.

**Coercion and Vote Buying**

A coerced voter may be able to provide proof of how they voted using an indirect voter association.

**Eligibility Tampering**

Because indirect voter associations are used to confirm eligibility, if an attacker has access to the IVA database, they may be able to maliciously modify the eligibility of ballots.

**Mitigations**

**Ensure Unlinkability of Ballots**

Ensure that the voting system does not receive any voter information that can be used to link a voter to their ballot selections. This might require provisional ballots to be submitted through the use of a paper ballot and follow a process external to the voting system to ensure no IVAs are stored within the voting system.

**Separate/External Storage**

This may done by storing the indirect voter associations in a database that is separate from the voting system. This could be a separate system to handle conditional ballots.
Related Requirements

Transparency Guideline 3.3
The public can understand and verify the operations of the voting system throughout the entirety of the election.

Interoperability Guideline 4.1
Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

Interoperability Guideline 4.2
Standard, publicly-available formats for other types of data are used, where available.

10.2.1 – Voter associations

10.2.1-A – Direct voter associations
The voting system must not create or store direct associations between a voter’s identity and their ballot.

Discussion
A direct voter association would be the voting system storing that John Smith voted for George Washington. Other examples of a direct association would include tying ballot selections to a social security number, voter identification number, or driver’s license number. (This is not an exhaustive list of direct voter association examples.)

10.2.1-B – Indirect voter associations
Only E2E voting systems may use indirect associations; other systems must not.

Discussion
Certain channels of voting require indirect associations so that ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. Once a ballot is read and counted, the ballot is permanently stripped of its identifier. The most common example of indirect association would be a randomly generated number. Ballots with indirect associations are not considered read or counted until the association is removed.

Applies to: E2E voting system architectures

10.2.1-C – Use of indirect voter associations
The voting system must only use indirect associations for situations when a voter needs to fill out a ballot before their eligibility is determined.

Discussion
Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. The act of casting the ballot permanently strips it of an identifier.

The most common example of indirect association would be a randomly generated number. Ballots with indirect associations are not considered cast until the association is removed.

Best practice would ensure that indirect voter associations are only available to authorized election personnel.

Applies to: 
E2E voting system architectures

10.2.1-D – Election worker selection of indirect associations
When the use of an indirect association is needed, an election worker must select the option for using an indirect association at the beginning of each new voting session.

Applies to: 
E2E voting system architectures

10.2.1-E – Isolated storage location
Ballots that are not cast and contain an indirect association must be stored in separate storage locations from cast ballots.

Discussion
Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast.

Applies to: 
E2E voting system architectures

10.2.1-F – Confidentiality for indirect association
Ballots that are not cast and contain an indirect association must be encrypted.

Discussion
Encryption of the ballot preserves the confidentiality of the voter’s ballot selections while the ballot is tied to an indirect association to the voter.

Applies to: 
E2E voting system architectures
10.2-D – Prohibition on voter record order information
The voting system must not contain data or metadata associated with the CVR and ballot image files which can be used to determine the order in which votes are cast.

10.2-E – Identifying information in voter record file names
CVR and ballot image names must not include any information identifying a voter.

Discussion
This helps to ensure that information that could accidentally be used to reference a voter is not used within a file name.

10.2-H – Aggregation and ordering
Aggregated and final totals must not contain voter specific information, and must not be able to recreate the order in which the ballots were cast.

10.2-J – Voting information with receipts
Receipts produced by a voting system must not contain voter information.

10.2-L – Activation device records
Activation devices must not create or retain information that can be used to identify a voter’s ballot, including the order and time at which a voter uses the voting system.

Discussion
The activation device must not create or retain any information that could be used for the purposes of identifying a voter’s ballot, or the time the voter arrived at the polls, or the specific vote-capture device used by the voter.

10.2-O – Ballot secrecy for receipts
The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

Applies to: E2E voting system architectures