Table.1: Fixes/improvements done in IVXV 1.9.10 EP2024

Risk	Deployed Solution	Remaining Issues	GiHub File	Corresponding Academic Research
Invalid votes	Decrypted in a separate file with ZKPs of correct decryption	-Files are viewable by auditors only (complaints) -Better deploy ***Range Proofs*** to prevent invalid votes from entering list.	Embedded in [42] ***DecryptTool.java***	Tallinn Univ. Ms. thesis [17] (Jun 2024)
Ballot Processor (BP) manipulation	Consistency checks on SHA256 hashes of totals and subtotals.	***Offline*** checks; i.e., count based validation depends on trusting the Vote Collector (VC) and Registration Service (RS) to not collude before the list enters the BP	A new file [45] ***IntegrityTool.java***	Tallinn Univ. researchers [46] (Dec 2024)
Timing attacks	Checking *Session ID* and *Timestamps* difference, which are generated by *PKIX* protocol	Cannot detect fast attacks that can manage to work in the duration of one session (like ***Pereira attack*** [35])	A new file [50] ***client.go***	An extension, [48], to a Luxemburg Univ. PhD on formal verification of i-voting systems, applied to IVXV (Jun 2024)

Table.2: Remaining vulnerabilities/risks in IVXV 1.9.10 EP2024 and suggested solutions

Vulnerability	Risks/threats	Concerns/Complaints about the issue	Suggested Solutions	Proposed by
Invalid votes	Privacy attacks [43]	Many persisting complaints for viewing their decryption files [14], concerned OSCE/ODHIR too [9]	Deploy ***Range Proofs*** to prevent invalid votes from entering the ballot list at all	Tallinn Univ. Ms. thesis [17] (Jun 2024)
Authenticating the Voting Application (VA)	-Pereira attack [35] -Copy attack on Privacy [48] -Large-scale vote buying/coercion through *encrypted copy attack* + PC execution attests + online coding to automate execution [88,89] -Variety of malicious VA risks	-Cybernetica supervised PhD [32/sec.5-6] -Olivier Pereira [35] -OSCE/ODHIR 2023 report [2] -Many other researchers including the authors of this paper.	Using a ***microcontroller*** voting device	Tallinn Univ. PhD [32] (2022)
			-Optional checking of ***file hash*** in an *Electrum* Bitcoin wallet style [55], but batched into 1 click [56] -Assigning a ***signature key*** for VA, and allowing ***optional registering of other VAs*** but after scanning the code for malicious activities (more robust, but require flexibility and cooperation from authorities to not reject unobjectively)	This paper
Insiders' Trust	VC and RS are trusted to not collude; their collusion may result in: -privacy attacks [43] - different possible manipulations of the ballots list before entering the ballot processor	-Estonian parties and i-voting opposing communities in general [1,2,13,19] -Detected by automated formal verification tools in [48]	-Adding a ***ZKP*** to each vote.	[43] (2022)
			-Performing different ***consistency check queries***, and ***RLA***s, between ballots list and other services recording digital transactions in Estonia, like *myID* [47]. -Using ***Verkle Trees*** [64] to cryptographically prove count values.	This paper
Absent Voters	If their devices (and credentials) are compromised as *botnets* or any dark web market, they can be subject to all nonverifying voters attacks. In addition, we have no clue on what to check here.	-Falls under un*avoidable risks that can't be performed on large-scale* by [32, 32/ref.166] since it will cause "observable anomalies" -Falls under (*corrupted voter device+ corrupted communication network*) category detected in [48]	Only safeguards, no complete protection [65/Appendix C]: -Activate an ***SMS ack*** with every digital card transaction on election days; could be delayed as discussed in [35]. -use a SNARK that supports ***Non-inclusion proofs***, and check RLA samples; voters could lie to falsify elections. -Allow a ***"reject all" choice*** to incentivize even boycotters to vote	This paper