Developing a Personal Voting Machine for the Estonian Internet Voting System

Valeh Farzaliyev[1,2,3], Kristjan Krips[1,3], and Jan Willemson[1,2]

[1]Cybernetica, Narva mnt 20, Tartu, Estonia
[2]STACC, Narva mnt 20, Tartu, Estonia
[3]Tartu University, Inst. of Comp. Sci., Narva mnt 18, Tartu, Estonia

Abstract

As the world's population is increasingly mobile, remote voting becomes more and more a necessity. Vote casting by paper mail is slow, expensive and error-prone. Voting over Internet, on the other hand, is a subject to a wide range of cyber attacks. One of the weakest points in current Internet voting (i-voting) schemes is the end user environment that is hard to control against both vote integrity and privacy attacks. The essence of the problem is that conventional end user devices (PC-s, mobile phones, etc.) are in some sense too powerful, being able to run malware without the voter having efficient means to detect it.

In the current paper, we propose a solution to this problem by introducing a single-purpose user-controlled voting device built on top of a microcontroller platform. We take the Estonian i-voting protocol as the example use case and build an independent client for it that runs on the ESP32 platform. As a by-product, we will also release the first open-source voting client for the Estonian i-voting protocol.

1 Introduction

The primary goal of elections is to adequately reflect political preferences of the electorate. Reaching this goal relies on the election organisers' ability to guarantee integrity of the ballot boxes and transparency of the counting process.

In case of electronic (and especially remote electronic) voting, the nature of such guarantees differs substantially from the paper voting. To start with, there is not even necessarily a physical ballot box that everyone can look at. To compensate for that, a number of verification mechanisms have been proposed [3]. These can be used to verify different claims about the integrity of the vote and tally [34].