An Investigation Into Worldwide Electoral Systems and the Development of a Novel Internet Voting System

Florian, Andrei (School: Saint Aidans C.B.S)

Democratic elections are the instrument that enables people to select representatives to advocate for their beliefs. Distrust in elections is reflected in a steady decrease in voter turnout and increase in anti-democratic movements worldwide. The primary problem electoral systems face is that their means of guaranteeing the secret ballot results in an inability to incontestably prove electoral integrity – a voter receives no guarantee that the vote they cast has been tabulated correctly. Recent breakthroughs in cryptography can be used to achieve ballot secrecy while allowing for the indisputable verification of an election's integrity. Such breakthroughs lead to the development of internet voting – the ability to cast votes using personal computing devices. Although such implementations can have many benefits, guaranteeing the security of such systems is considered an insurmountable obstacle due to the inherent security vulnerabilities in voter hardware. Due to security concerns, internet voting is considered inappropriate for use in high-stakes elections. I propose an innovative internet voting solution that provides full-stack security and adheres to end-to-end verifiability standards. The inevitable security vulnerabilities in voter hardware are circumvented through the implementation of a hybrid system which involves casting ballots through the introduction of encrypted candidate selections from posted paper ballots into personal computing devices. My solution allows third parties to independently verify the integrity of an election at all stages while persisting voter anonymity. The innovative methodologies employed in this application achieve unparalleled security and form the basis of a novel end-to-end verifiable internet voting application.

Awards Won:

First Award of $5,000

Oracle Academy: Award of $5,000 for outstanding project in the systems software category.