Initial Project - Secure voting

Author: Scott Hulbert
Supervisor: Dr George Theodorakopoulos - Senior Lecturer
Module: CM3203 - 40 credits

Project Description

This project aims to create a secure voting application. Electronic voting is a well-documented and well-researched area. There have been strong arguments both for and against electronic voting. This project aims to investigate some of the ethical and technical challenges faced by electronic voting and how blockchain may be used to address some of these challenges.

A user of the application should be able to cast an anonymous vote. No unauthorized party should be able to vote on behalf of an authorized voter. To achieve this, the application needs to be able to authorise legitimate voters and reject everybody else.

To understand what is meant by a secure voting system, we should define what we mean by secure in terms of the security properties the voting application should have.

The security properties that should be considered are:

- Confidentiality - No person can tell how another person voted
- Integrity - No person can modify or delete a vote nor can they insert a false vote into the system
- Authentication - Only authorized parties can vote
- Anonymity - It is not possible to tie someone’s identity within the voting system to their real life identity

It would be desirable for the project to implement all of these properties but this may prove challenging. For example, in a decentralised system, it seems challenging to provide both anonymity and authentication as they appear at odds with each other. If a centralised approach is taken, then the system may implement all these properties at the cost of there being a central authority.

This will be achieved by implementing a voting system and evaluating its security. This will be done by both discussing the security of the technologies used and, if there is time, attempting to break the system. The initial implementation will likely be command-line based, due to the focus of the project being to create a blockchain for the storing of votes. If time permits, a web interface will be developed, to allow the system to be more accessible.

Project Aims and Objectives

Must do:

- Understand the landscape of voting systems and blockchains
    - Investigate the options available for creating private blockchains (e.g. Hyperledger)
    - Investigate recent research about voting systems - particularly voting systems that make use of blockchains, public and private

- Design a blockchain for storing user votes securely
- Implement the vote blockchain

- Evaluate the theoretical security of the voting system
    - What security properties does/doesn't the vote blockchain have?

- Evaluate the performance of the voting system
    - How does the system scale in respect to number of voters?
    - What size elections (e.g boardroom, general election) could the system reasonably support?
    - How could the performance of the system be improved?

Should do:

- Design a web application frontend that the user will cast votes on
- Design the backend supporting the web application that handles processing votes

- Implement the web application and it's backend

- Identify what security properties the web application does/doesn't have

Might do:

- Pentest the voting system to evaluate the practical security
    - Attempt common attacks against the website (SQL Injection, XSS, Brute Force)
    - What security properties can an attacker break with access to the system?
    - Design and implement attacks to exploit security properties the system lacks

- Improve the voting system
    - Design security improvements to the system that address the findings from pentesting
    - Implement those security improvements
    - Repeat attacks

Work Plan

Deliverables:

- Implementation of a blockchain-based voting system
- Explanation of the implementation
- Performance and security evaluation of the implementation

Week 1 ending 4/2/19:

- Focus on writing initial plan

Week 2 ending 11/2/19:

- Work on understanding blockchains
    - Investigate Hyperledger frameworks (Fabric, Sawtooth, Burrow)
    - Understand the differences between them

Week 3 ending 18/2/19:

- Continue work to understand blockchains
    - Pick a framework to start experimenting with
    - Set up a 4 node cluster
- Look at the research landscape of voting systems using blockchain
    - Find examples of voting systems using public blockchains such as Ethereum
    - Find examples of voting systems using private blockchains such as the Hyperledger frameworks
    - Identify strengths and weaknesses of public and private blockchain voting systems

Week 4 ending 25/2/19:

- Identify the framework to implement the vote blockchain in
- Design the structure of the blockchain
- Review meeting with supervisor to discuss the blockchain framework and structure chosen
- Begin work on implementing the blockchain

Week 5 ending 4/3/19:

- Continue work on implementing the blockchain

Week 6 ending 11/3/19:

- Continue work on implementing the blockchain
- Begin evaluating the security and performance of the blockchain

Week 7 ending 18/3/19:

- Continue evaluation of the security and performance of the blockchain
- 2nd review meeting to discuss the implementation, security properties and performance evaluation of the blockchain

Week 8 ending 25/3/19:
- Design a web application to allow users to access the blockchain from a web browser
- Start implementing the web application

Week 9 ending 1/4/19:
- Continue implementing the web application

Week 10 ending 8/4/19:
- Evaluate the security of the web application and its backend
- 3rd review meeting with supervisor

Week 11 ending 15/4/19:
- Work on finalising report
- Prepare for demonstration of voting system

Work Plan Notes:
- By the end of week 7, I aim to have completed my ‘Must Do’s and have them documented in the report
- By the end of week 10, I aim to have completed my ‘Might Do’s and have them documented in the report

- If I am ahead of the plan, I will start the work for the next week
- If I am behind, I will delay starting the work for the week until I have finished the work for previous weeks
- If I complete all the items on the plan before the end of week 11, I will start work on the ‘Might do’s
- I have not included my ‘Might do’s in the plan as I do not anticipate finishing the entire plan early.

- I have not planned anything for the Easter break period, this is for two reasons:
  - To allow myself to focus on revision in the examination period
  - To allow myself some buffer time, in case things don’t go to plan, I will have this time to catch up

- I may make use Kanban boards to keep track of tasks

- I would use one Kanban board for the tasks listed above with a simple To-do/Doing/Done columns - this would help me break down each task in the plan into smaller components
- Another Kanban board to keep track of development tasks with Design/Develop/Test/Deploy columns

- I will have weekly meetings with my supervisor to discuss my progress in addition to the review meetings I have scheduled in weeks 4, 7 and 10
- I will write the report for the project as I work through the items - I will aim to leave one day at the end of the week for report-writing