Modeling Conflicts in Secret Ballot Elections

Aaron Wilson, CIS Sr. Director of Election Security
E-Vote-ID, October 2, 2019
A Little About Me

- I like
  - Building things
  - Solving problems
  - Security
  - Election technology

- Sr. Director of Election Security, CIS
- Director of Product Innovation, Clear Ballot Group
- Vice President of Product, Greenshades Software
- Project Engineer, Scytl
- Computer Programmer, Florida Division of Elections
Quick Outline

MOTIVATION AND APPROACH
DEFINITIONS
CONFLICT MODEL AND DISCUSSION
That would work, but….

I have this great idea on how to build a voting system

No, seriously, let me explain it again.

That would work, but…

How much time do you have for me to explain this?
Not your normal requirements

• Trade-offs are typical, but there is something unique about e-voting

- **Quantity**
  - Number of conflicts

- **Intensity**
  - Legal constraints, passionate groups
How this work can be helpful

Don’t get trapped in the maze
Navigate without retracing steps

Might make something un-fieldable
Keep conflicts in mind when solving problems

Don’t make ill-informed architecture decisions
Select the right approach/technology from the start

Don’t overpromise
Set proper expectations
Requirements Engineering (RE) Conflict Management

- Conflict Identification
- Conflict Analysis
- Conflict Resolution
Goal Modeling Approach

- Higher level of abstraction than requirements
- Provide context between business context and requirements
- Enables goal-oriented requirements engineering
- Provide implementation and conflict resolution flexibility
Identification and Classification

- **Identification**
  - Manual over automated technique
  - Looked at real and proposed e-voting applications

- **Classification**
  - Interference – negative contribution of one goal on another (strong)
  - Divergence – some combination of circumstances makes the goals conflicting (weak)
Secret Ballot

- **Secret Ballot Goal**
  - Voter Anonymity
  - Coercion-Resistance
One Person One Vote Goal

- Voter Authenticity
- Ballot Accountability
Universal Access

• **Universal Access Goal**
  – Voter Usability
  – Voter Accessibility
  – Provisional Voting
Transparent and Auditable

- Transparent and Auditable Goal
  - Cast as Intended Verifiability
  - Recorded as Cast Verifiability
  - Tallied as Recorded Verifiability
## Conflict Identification

<table>
<thead>
<tr>
<th>Goal</th>
<th>Goal</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voter Authentication</td>
<td>Voter Anonymity</td>
<td>Interference</td>
</tr>
<tr>
<td>Voter Authentication</td>
<td>Voter Usability</td>
<td>Interference</td>
</tr>
<tr>
<td>Voter Anonymity</td>
<td>Voter Accessibility</td>
<td>Divergence</td>
</tr>
<tr>
<td>Coercion Resistance</td>
<td>Voter Usability</td>
<td>Interference</td>
</tr>
<tr>
<td>Coercion Resistance</td>
<td>Cast as Intended Verifiability</td>
<td>Divergence</td>
</tr>
<tr>
<td>Coercion Resistance</td>
<td>Recorded As Cast Verifiability</td>
<td>Divergence</td>
</tr>
<tr>
<td>Provisional Voting</td>
<td>Voter Anonymity</td>
<td>Divergence</td>
</tr>
<tr>
<td>Cast as Intended Verifiability</td>
<td>Voter Usability</td>
<td>Interference</td>
</tr>
<tr>
<td>Cast as Intended Verifiability</td>
<td>Voter Accessibility</td>
<td>Interference</td>
</tr>
<tr>
<td>Recorded as Cast Verifiability</td>
<td>Voter Anonymity</td>
<td>Divergence</td>
</tr>
<tr>
<td>Tallied as Recorded Verifiability</td>
<td>Voter Anonymity</td>
<td>Divergence</td>
</tr>
</tbody>
</table>
Conflict Model

<table>
<thead>
<tr>
<th>Goal</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voter Anonymity</td>
<td>5</td>
</tr>
<tr>
<td>Coercion Resistance</td>
<td>3</td>
</tr>
<tr>
<td>Cast as Intended Verifiability</td>
<td>3</td>
</tr>
<tr>
<td>Voter Usability</td>
<td>3</td>
</tr>
<tr>
<td>Voter Accessibility</td>
<td>2</td>
</tr>
<tr>
<td>Recorded as Cast Verifiability</td>
<td>2</td>
</tr>
<tr>
<td>Tallied as Recorded Verifiability</td>
<td>1</td>
</tr>
<tr>
<td>Provisional Voting</td>
<td>1</td>
</tr>
</tbody>
</table>
Voter Authentication Interferes with Voter Anonymity

• **Analysis**
  – Voter anonymity is best accomplished in a system where the identity of the voter is never introduced for any purpose.
  – Voter authentication requires the voter identity to be proven

• **Examples**
  – Two-agency systems
  – Postal voting
  – Digital two-envelope systems

• **Classification**
  – Interference – fundamental conflict, only mitigated through trust in people and processes
Coercion Resistance Interferes with Voter Usability

• Analysis
  – Voting in the most straight forward, usable manner allows a coercer the opportunity to simply observe the act of voting
  – In-person voting can be coercion resistance without hurting voter usability, but still must not allow proof to be taken

• Examples
  – JCJ
  – Civitas

• Classification
  – Interference – we don’t have good mitigations. Multi-voting, real/fake ballots both hurt usability
Cast as Intended Verifiability Interferes with Voter Usability

• Analysis
  – Voter-initiated verification requires extra steps in the voting process
  – Usability is hurt by extra steps, especially non-traditional steps which may confuse the voter

• Examples
  – Prêt à Voter
  – PunchScan

• Classification
  – Interference - no current implementation without an extra, undesirable step in the voting process
Provisional Voting Diverges with Voter Anonymity

• Analysis
  – Provisional balloting requires ballots be held separate from counted ballots and stay associated with the voters so it can be identified

• Examples
  – Direct Recording Electronic
  – Blockchain Systems

• Classification
  – Divergence – limited to electronic systems, some effective mitigations
Conclusions

- Performed conflict identification, analysis, and development of a conflict model
- The model can be used to evaluate current implementations
- Assist is making critical decisions early in the process
- Future Work
  - More formal conflict analysis and resolution
  - Expand model to more than pair-wise conflicts
Thank You!

Aaron Wilson

Aaron.Wilson@cisecurity.org
Why this topic?

- To better understand these conflicts myself
- Give others a starting point
- Evaluations of implementations