PRÊT À VOTER

MSc Group Project Presentation
OVERVIEW

Prêt à Voter

• **Anonymous** - voter identity protected, coercion resistant

• **Secure** - tamper resistant, minimum operating trust

• **Verifiable** - built-in auditing capabilities, public transparency

Unusual combination of anonymity and ability to be audited
ELECTIONS ARE BROKEN

13%

Average turnout*

*src: Exeter University ‘Average UK student election turnout’
ELECTIONS ARE BROKEN

• Low turnout
• Inaccessible
• Costly infrastructure
• No public auditing
• Tangled trust structure

E-voting was supposed to solve these problems, but poor implementations have lead to a lack of trust
VOTING PROCESS

1. Eligibility
2. Ballot
3. Casting
4. Counting
Authentication:

- Fully modular - plug in the level of security you need
- Kerberos used within DoC

Token generation:

- Anonymous - no identity matched to a token
- One-time use
- Tied to an election
Ballot generation:

- Candidate list permuted by random cyclic-shift
- Unique hash value generated via one-way function
- Onion core created to store hash and cyclic-shift offset
- Onion layers added, encrypting at each step with public keys
- Encrypted Onion stored in database
<table>
<thead>
<tr>
<th>Canonical list</th>
<th>Potential ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clare</td>
<td>Kacper</td>
</tr>
<tr>
<td>Jibran</td>
<td>Matt</td>
</tr>
<tr>
<td>Kacper</td>
<td>Clare</td>
</tr>
<tr>
<td>Matt</td>
<td>Jibran</td>
</tr>
<tr>
<td>-</td>
<td>FC56-GHFD-5GFH</td>
</tr>
</tbody>
</table>

Individual ballots are unpredictable
No single entity can decode a ballot
Vote recording:

- Candidate number and unique hash stored in database
- User receipt provided for public verification of vote
- 2D barcode generated for convenience

You voted for number 2

FC56-GHFD-5GFH
<table>
<thead>
<tr>
<th>Eligibility</th>
<th>Ballot</th>
<th>Casting</th>
<th>Counting</th>
</tr>
</thead>
</table>

### Vote Batching:
- Onions batched by database and sent to Tellers
- Onion layers removed and core passed to Counter

### Vote Counting:
- Vote for matching hash requested from database
- True vote calculated from offset and registered to candidate
CLIENT-SERVER

- Model View Controller
- Multi-layer architecture
- Concern separation

Separation of concerns leads to cleaner more efficient code
DEMO
LEARNINGS

Security

Distributed systems

Web programming
Anonymous  ●  Secure  ●  Verifiable