Cobra: Toward Concurrent Ballot Authorization for Internet Voting

Aleksander Essex, Jeremy Clark, & Urs Hengartner
End-to-End Verifiable Voting

- Verifiably correct tally
- Ballot secrecy
End-to-End Verifiable Voting

- Verifiably correct tally
- Ballot secrecy

Internet Voting

- Coercion & vote selling
- Untrustworthy platform
  - Denial of service
Coercion & Vote Selling

JCJ, Civitas, Selections, Araujo et al., Spycher et al.
Coercion & Vote Selling

JCJ, Civitas, Selections, Araujo et al., Spycher et al.

Untrustworthy Platform

SureVote, Code Voting, Pretty Good Democracy, Remotegrity
Coercion & Vote Selling

JCJ, Civitas, Selections, Araujo et al., Spycher et al.

Untrustworthy Platform

SureVote, Code Voting, Pretty Good Democracy, Remotegrity
Coercion & Vote Selling

JCJ, Civitas, Selections, Araujo et al., Sypcher et al.

Untrustworthy Platform
SureVote, Code Voting, Pretty Good Democracy, Remotegrity

Denial of Service Attacks
Application layer flooding
Coercion & Vote Selling

JCJ, Civitas, Selections, Araujo et al., Spycher et al.

Untrustworthy Platform

SureVote, Code Voting, Pretty Good Democracy, Remotegrity

Cobra

Denial of Service Attacks

Application layer flooding
Coercion-Resistance

A voter can convince an adversary she voted for Alice while actually voting for Bob
• Voters choose a password that allows them to vote during registration
• The password scheme has a simple cognitive rule for creating fake (“panic”) passwords
• Fake passwords can be sold or supplied under coercion
• The system will accept votes with fake passwords, but these votes will be obliviously canceled out
• Voters can vote with their real password any time. This ballot is unlikable to any ballots they cast with fake passwords
• Voters choose a password that allows them to vote during registration
• The password scheme has a simple cognitive rule for creating fake (“panic”) passwords
• Fake passwords can be sold or supplied under coercion
• The system will accept votes with fake passwords, but these votes will be obliviously canceled out
• Voters can vote with their real password any time. This ballot is unlikable to any ballots they cast with fake passwords
Denial of Service

- Application-layer flooding
- Concurrent ballot authorization
Roster

Concurrent BA

Concurrent BA

Concurrent BA

Homomorphically Sum
Work done by election authority
Work done by election authority
Roster

Concurrent BA

Concurrent BA

Concurrent BA

Concurrent BA
Fundamental Mechanism

• Private Set Membership
Is encrypted password $[p]$ on the roster?
Is encrypted password $[p]$ on the roster?

No: $[0] \times [v] = [0]$

Yes: $[1] \times [v] = [v]$
Is encrypted password \( p \) on the roster?

Plaintext equality tests & polynomials:
Encrypted Bloom Filters
0 1 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0 0 1 0 0 1 0 0 0
a

H₁ → [0] → [3]

H₂ → [1] → [0]

H₃ → [2] → [0]

0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0
Cobra
• Voters’ (obfuscated) passwords are added to an encrypted Bloom filter during registration

• See paper for details

• Properties:
  • Registrar does not see obfuscated password
  • Publicly verifiable proof that each voter added only a single entry
  • Coercion-resistant
\(< g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) >\)
\(< g^p, [v], PoK(p: g^p), PoM(v) >\)

Check Proofs

\(< g^p, [v] >\)
\(< g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) >\)
< g_p, [v], PoK(p: g_p), PoM(v) >

Query(g_p)

< [1], [v] >
\[ < g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) > \]

Mix & Match:

\[
\begin{array}{cc}
[0] & [0] \\
[1] & [v]
\end{array}
\]
\[ \langle g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle \]

\[ \langle g^p, [v] \rangle \]

\[ \langle [0], [v] \rangle \]

\[ \langle [0] \rangle \]

Mix & Match:

\[
\begin{array}{cc}
[0] & [0] \\
[1] & [v] \\
\end{array}
\]
See paper for more:

- **Registration**: setting up the Bloom filter (*expensive!*); setting false positive rate
- **Optimizations**: using BGN to eliminate steps
- **Security analysis**: eligibility verification, integrity, coercion-resistance
- **A blueprint** that might be useful for concurrent ballot authorization other ways
Table 1: Performance comparison in number of modular exponentiations for a moderately-sized election scenario: 5 candidates, 10,000 registered voters, 20,000 submitted ballots, and 3 trustees.
Concluding Remarks

- **DOS** on internet voting is a reality
- Common properties of coercion-resistance systems (anonymous ballot submission, intensive post-tally processing) make protocol-level DOS a threat
- We have shown in principle ballots can be authorized concurrently (and incidentally post the fastest tally with Cobra)
- **Future work:** speed-up registration
Questions?

@AleksEssex
@PulpSpy
@uhengart