NTNU

Innovation and Creativity

Security Aspects of Internet-based Voting

Md. Abdul Based
Department of Telematics

December 7, 2011

Outline

- Security Requirements of Internet Voting
- The Voting Scheme
- Summary and Future Plan

NTNU
Innovation and Creativity

Security Requirements of Internet Voting

- Basic Requirements
- Enhanced Requirements

NTNU
Innovation and Creativity

Basic Requirements

- Eligibility of the Voter
- Confidentiality of the Ballot
- Integrity of the Ballot
- Privacy and Secrecy
- Robustness
- Fairness
- Soundness
- Completeness
- Unreuseability of the Ballot

NTNU
Innovation and Creativity

Enhanced Requirements

- Unlinkability and Untraceability
- Validity of the Ballot
  - Interactive Zero-Knowledge Proof Protocol
  - Non-interactive Zero-Knowledge Proof Protocol
- Verifiability
  - Universal/Public Verifiability
  - Voter Verifiability
- Receipt-freeness
- Coercion-resistance

NTNU
Innovation and Creativity

The Voting Scheme

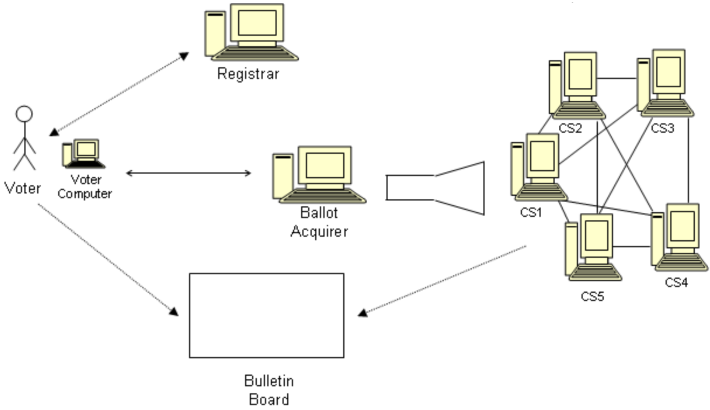


Figure: The Voting Scheme

NTNU
Innovation and Creativity

The Protocol between the Voter and the Registrar

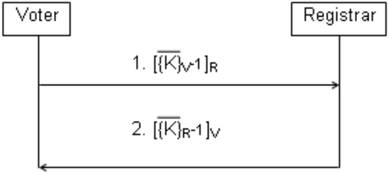
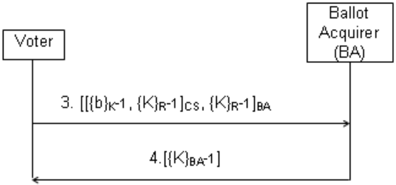

Voter
Registrar
1. $[\overline{\{K\}}_{V^{-1}}]_R$
2. $[\overline{\{K\}}_{R^{-1}}]_V$

Figure: Protocol between Voter and Registrar

NTNU
Innovation and Creativity

The Protocol between the Voter and the Ballot Acquirer



Voter

Ballot Acquirer (BA)

3. $[[\{b\}_{K-1}, \{K\}_{R-1}]_{CS}, \{K\}_{R-1}]_{BA}$

4. $[\{K\}_{BA-1}]$

Figure: Protocol between Voter and Ballot Acquirer

NTNU
Innovation and Creativity

The Protocol between the Voter and the Bulletin Board

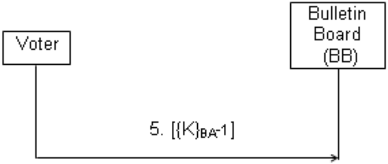


Figure: Protocol between Voter and Bulletin Board

The Protocol between the Ballot Acquirer and the Counting Server

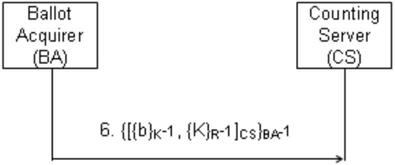
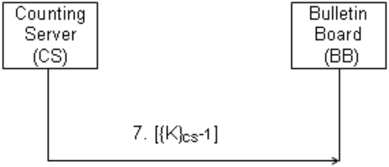


Figure: Protocol between Ballot Acquirer and Counting Server

The Protocol between the Bulletin Board and the Counting Server



Counting Server (CS)

Bulletin Board (BB)

7. $[\{K\}_{cs\text{-}1}]$

Figure: Protocol between Bulletin Board and Counting Server

Security Analysis (Informal)

- Eligibility
- Confidentiality and Integrity of the Ballot
- Privacy and Secrecy
- Robustness and Fairness
- Soundness, Completeness, and Unreuseability of the Ballot

NTNU
Innovation and Creativity

Security Analysis (contd.)

- Unlinkability and Untraceability
- Validity of the Ballot
- Voter Verifiability
- Universal Verifiability
- Receipt-freeness and Coercion-resistance

NTNU
Innovation and Creativity

Summary and Future Work

Summary

- The Voting Scheme satisfies the basic and enhanced requirements

Future Plan

- Formal Analysis

NTNU
Innovation and Creativity

- Thank You.
- Comments and Questions!

NTNU
Innovation and Creativity