Elektronické voľby pre malý počet hlasujúcich

Marián Horňák
školiteľ: Doc. RNDr. Daniel Olejár, PhD.

30. August 2017

Motivácia

Primárnou motiváciou pre prácu bolo elektronické hlasovanie v nasledovných situáciách:

- hlasovanie v akademickom senáte,
- diaľkové hlasovanie pri obhajobách;

sekundárnou motiváciou bolo zistenie, že elektronické hlasovanie v reálnom čase, je veľmi slabo pokryté výskumom.

Ciele

Z motivácie vyplynuli nasledovné ciele práce:

- Navrhnúť elektronický systém vhodný pre hlasovanie malej skupinky účastníkov v reálnom čase
- Vykonať bezpečnostný rozbor systému, stanoviť podmienky pre správne fungovanie
- Dosiahnuť podmienky porovnateľné alebo lepšie ako pri klasickom hlasovaní s urnou a plentou

Bezpečnostné vlastnosti hlasovania

Overiteľnosť – Účastníci si môžu overiť, že hlasovanie prebehlo správne, najmä:

- **Individuálna overiteľnosť** – Autor si môže overiť, že jeho hlas bol zarátaný.
- **Všeobecná overiteľnosť** – Všetci si môžu overiť, že sčítanie prebehlo správne.
- **Overiteľnosť platnosti** – Všetci si môžu overiť, že hlasovali práve tí, čo mali.

Dôvernosť – Nikto okrem autora nie je schopný zistiť akúkoľvek informáciu o obsahu hlasu.

Nedokladovateľnosť – Autor nie je schopný formálne presvedčiť inú osobu o tom, ako hlasoval.

Významné historické práce

1994. Cramer, Damgård, Schoenmakers.
Proofs of partial knowledge and simplified design of witness hiding protocols.

1997. Cramer, Gennaro, Schoenmakers.
A secure and optimally efficient multi-authority election scheme.

2008. Adida.
Helios: Web-based open-audit voting

Nedávny výskum sa venuje prevažne nedokladovateľnosti a veľkoplošným voľbám, na ktoré v práci nenadväzujeme.

Modelová situácia

V prvej časti práce sme zhodnotili rôzne situácie vyžadujúce malé hlasovania a vytvorili modelovú situáciu, z ktorej sme neskôr vychádzali:

- najviac 100 hlasujúcich,
- najviac 10 dopredu známych kandidátov,
- dostupné mobilné zariadenia a jeden prenosný počítač,
- hlasujúci na diaľku,
- hlasujúci bez zariadenia,
- okamžité vyhodnotenie.

Navrhnutý protokol

Na základe modelovej situácie sme navrhli hlasovací protokol s nasledujúcimi vlastnosťami:

- založený na práci *A secure and optimally efficient multi-authority election scheme (1997)*,
- centrálny verejný komunikačný kanál – nástenka,
- autoritami sú hlasujúci so zariadením,
- overiteľný a dôverný,
- autentifikácia je otvorená,
- možnosť hlasovať bez zariadenia,
- webová aplikácia.

Hlasovanie bez zariadenia - princípy

Hlasujúci vytvorí a zverejnení hlas ešte pred hlasovaním. Počas hlasovania potom oznámi permutáciu (rotáciu) možností, tak aby zvolil želaného kandidáta. Jeho hlas sa následne prešifruje s využitím kľúčov špecifických pre dané hlasovanie, čím sa umožní jeho dôverné spracovanie.

Prešifrovanie vykonávajú účastníci so zariadeniami, ktorí sa takto môžu dozvedieť čiastočnú informáciu o hlase. Samotný hlas je však lineárnou kombináciou týchto informácií, takže bez spolupráce prekladateľov zostáva v utajení.

Hlasovanie bez zariadenia - bezpečná verzia

Hlasujúci bez zariadenia pri tejto alternatíve postupuje nasledovne:

- predpríprava hlasu doma,
- oskenovanie pripraveného hlasu (QR kód),
- hlasovanie podľa tajnej predtlačenej permutácie,
- oskenovanie tajomstiev rôznymi autoritami.

Hlasovanie je vždy overiteľné a dôverné, ak dostatok skenujúcich (škálovateľný k 1) je čestných.

Hlasovanie bez zariadenia - praktická verzia

Hlasujúci bez zariadenia pri tejto alternatíve postupuje nasledovne:

- dohoda s treťou stranou,
- predpríprava hlasu doma,
- oskenovanie pripraveného hlasu (QR kód),
- hlasovanie podľa tajnej predtlačenej permutácie.

Hlasovanie je vždy overiteľné a dôverné, ak je tretia strana čestná.

Výsledky

- Rozbor malých hlasovaní a zostavenie modelovej situácie.
- Návrh efektívneho protokolu s využitím dostupných zdrojov (realizovaný úpravou existujúcich riešení).
- Vlastné riešenia problému hlasujúceho bez zariadenia.
- Formalizácia navrhnutého protokolu.
- Architektonický návrh a čiastočná implementácia.

Ďakujem za pozornosť

K posudkom všeobecne

- Nedostatky vo formálnej úprave sú dôsledkom zlého rozdelenia práce medzi implementáciu a spisovanie.
- Sekcia 2.1 mala za úlohu v krátkosti predstaviť štandardné pojmy a odkázať na súvisiacu literatúru, preto niektoré pojmy neboli dodefinované.

K posudku školiteľa

- 4.c – Áno, výsledok hlasovania je realizácia funkcie.
- 5.a – Údaje vo formalizácii protokolu boli matematické objekty, ich formálnu špecifikáciu som považoval za implementačné rozhodnutie.
- 5.c – Normalizovanú analýzu bezpečnosti som plánoval v nadväznosti na implementáciu.

K posudku oponenta

- 2.a – Analýzu rizík z pohľadu východiskových situácií som čiastočne uvádzal pri návrhu, všeobecne som však robil iba analýzu z pohľadu bezpečnostných vlastností.
- 2.b – Odôvodnil som funkčnosť a bezpečnosť vlastných modifikácií, analýzu prevzatých častí protokolu som vynechal.
- 2.c – Nemyslím si, že by rozdelenie modelovej situácie znížilo komplexitu riešenia.
- 2.d – Vysokoúrovňové popisy protokolu sú uvedené pri návrhových rozhodnutiach.
- 3 – Uvedené identifikátory sú špecifikované do miery nevyhnutnej pre pochopenie protokolu s odkazom na ich možnú implementáciu.