Electronic Election System for Academic Senate

Adam Štefunko
Školiteľ: RNDr. Jaroslav Janáček, PhD.

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Jún 2018

Obsah

Definícia

Požiadavky

Základné typy

Existujúce systémy

Navrhovaný systém

Implementácia

Splnenie požiadaviek

Problémy a výzvy

Definícia

> **Electronic voting**, *a form of computer-mediated voting in which voters make their selections with the aid of a computer.* Britannica
>
> *...voting using electronic means to either aid or take care of the chores of casting and counting votes.* Wikipedia

Elektronický volebný systém je počítačový systém, ktorý

- autentifikuje voliča,
- umožní voličovi hlasovať,
- bezpečnečne prenesie a uloží hlas,
- spočíta hlasy.

Požiadavky

1. Použiteľnosť
   - ľahko použiteľné používateľske prostredie
   - mobilita
   - rentabilita
   - potvrdenie
2. Bezpečnosť
   - tajnosť
   - anonymita
   - spoľahlivosť
   - neovplyvniteľnosť
3. Presnosť
   - autorizácia
   - jedinečnosť a limitácia
   - stálosť
   - správnosť spočítania

Základné typy

Na základe použitej technológie:

1. E-Voting
   - špeciálne hlasovacie zariadenia
   - obmedzená mobilita
   - nízka zraniteľnosť, avšak potenciálne skryté hrozby
2. **I-Voting**
   - osobné počítače pripojené cez internet
   - skoro neobmedzená mobilita
   - zraniteľnosť závislá na jednotlivých zariadeniach

Existujúce systémy

- Estónsko
  - možnosť podpísať elektronické dokumenty cez občianske preukazy
  - dvojitá obálka
  - externé dešifrujúce a sčítacie zariadenie
- Nórsko
  - návratné kódy
  - externé dešifrujúce a sčítacie zariadenie
- Švajčiarsko
  - nutnosť zadať súkromné hodnoty
  - potvrdzujúce a ukončujúce kódy

Navrhovaný sytém

- podobný estónskemu systému
- **systém nevie nič o voličovi, keď je hlas dešifrovaný**
- **internetová aplikácia použitá na hlasovanie**
- možnosť upraviť hlas
- umožnenie papierového hlasovania
- fázy: *inicializácia*, *hlasovanie*, *sčítavanie*

Účastníci volebnej schémy

- Volič V
- Volebná komisia B
- Databáza D
- Volebná aplikácia A
- Server pre zber hlasov S
- Zariadenie na sčítavanie hlasov M
- Autentifikačná autorita T

Inicializácia

1. v databáze D vytvorená tabuľka kandidátov a voličov
2. vytvorený volebný verejný a súkromný kľúč
3. súkromný kľúč zdieľaný
4. verejný kľúč vložený do volebnej aplikácie

Hlasovanie

1. volič sa autentifikuje pomocou *UK loginu* a spustí sa volebná aplikácia
2. odošle sa volebný formulár a vytvorí sa a zašifruje hlas
3. hlas sa pošle serveru S
4. server S autorizuje voliča
5. ak volič predtým nehlasoval papierovo, hlas je uložený spolu s voličovým *UK loginon*
6. počas papierového hlasovania sa pošle špeciálny hlas zabraňujúci voličovi ďalej hlasovať

Sčítavanie

1. zašiforvané hlasy bez identít voličov sa prenesú do zariadenia M
2. hlasy sa dešifrujú, overia a sčítajú
3. publikujú sa výsledky

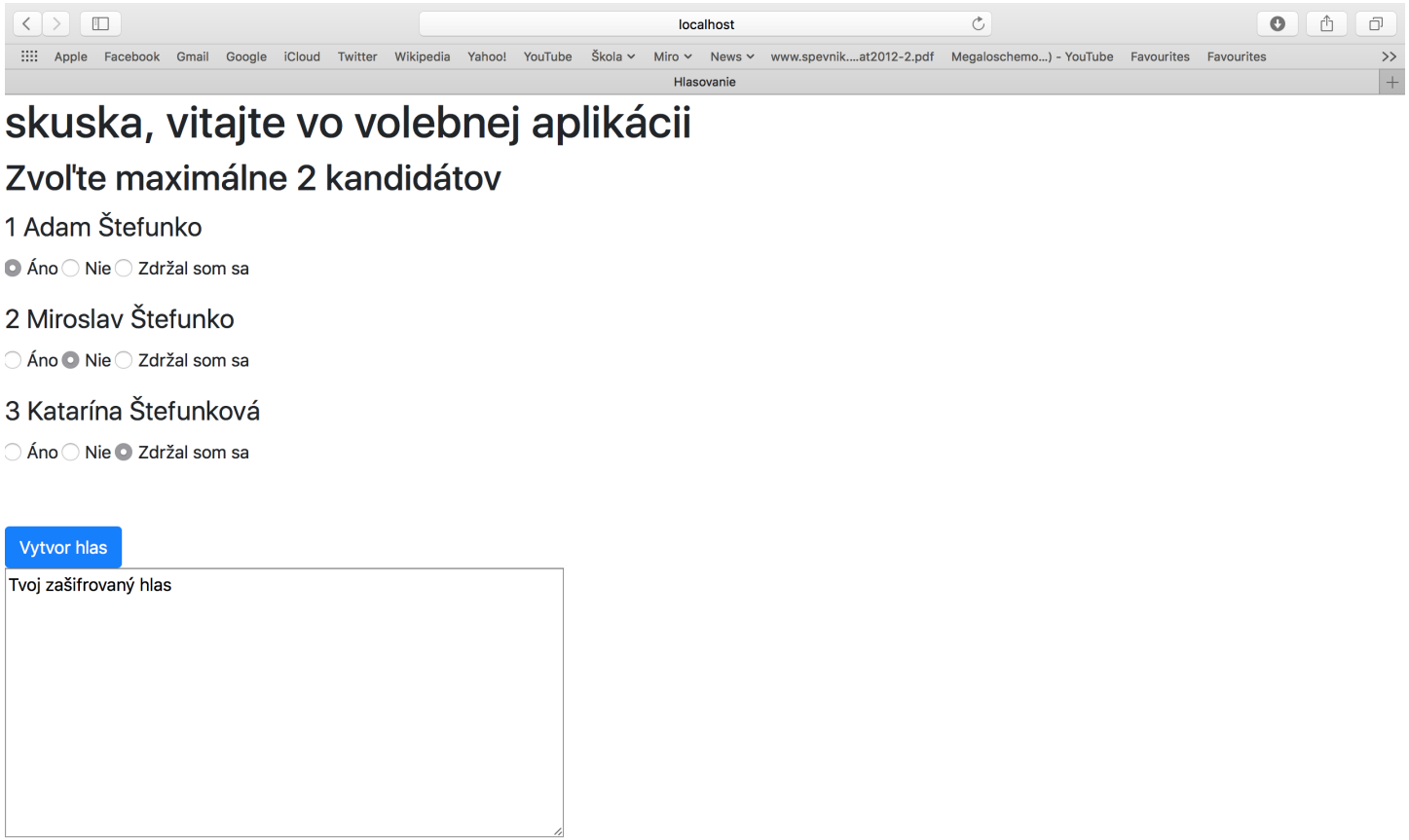
Použité technológie

- OpenPGP
  - šifrovanie a dešifrovanie hlasu
- Shamirova schéma na zdieľanie tajomstva
  - rozdelenie súkromného kľúča
- Cosign
  - jednotná autentifikácia používaná univerzitou

Implementácia

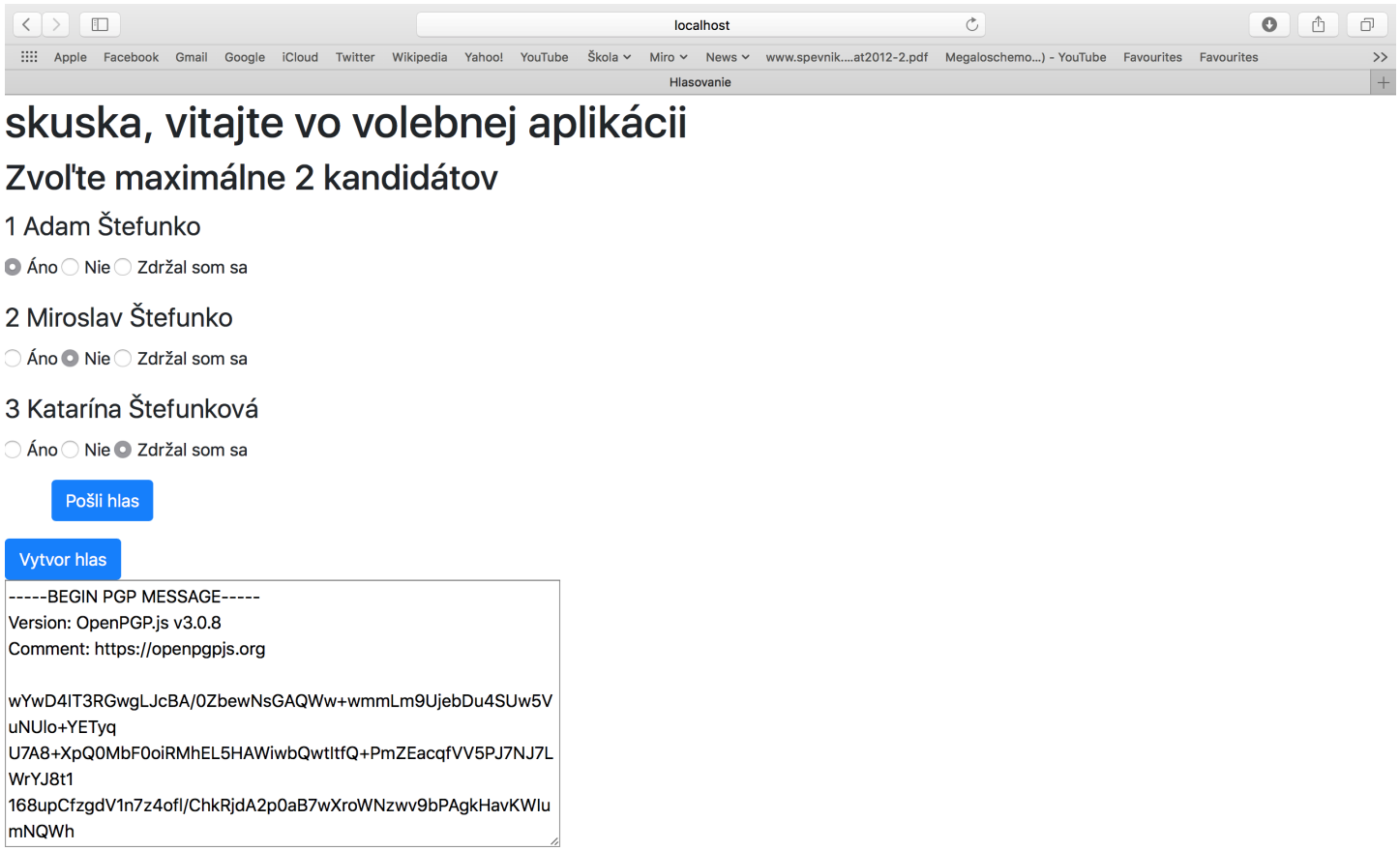
- Databáza: *SQL*
- Back end: *Python*
- Front end: *JavaScript*
- Volebný formulár: *HTML*
- spracovanie hlasu cez *CGI* skripty
  - server spúšťa kód volebnej aplikácie

Demoštrácia



Obr.: Hlasovací formulár

Demonštrácia



Obr.: Hlasovací formulár so zašifrovaným hlasom

Demonštrácia

Toto sú výsledky volieb:
Adam Štefunko Áno: 3 Nie: 0 Zdržali sa: 1
Miroslav Štefunko Áno: 1 Nie: 1 Zdržali sa: 2
Katarína Štefunková Áno: 1 Nie: 0 Zdržali sa: 3

Obr.: Výsledky

Splnenie požiadaviek

- ľahko použiteľné používateľské prostredie
- mobilita
- rentabilita
- potvrdenie
- tajnosť
- anonymita
- spoľahlivosť
- neovplyvniteľnosť
- autorizácia
- jedinečnosť a limitácia
- stálosť
- správnosť spočítania

Problémy a výzvy

- kompatibilita kryptografických knižníc
- zoznámenie sa a práca s knižnicami
- autentifikácia na univerzite

Budúce plány

1. doladenie častí implementácie
2. zavedenie systému a jeho testovanie na univerzite
3. prispôsobiteľnosť odpovedí
4. aplikácia pre smartfóny

Ďakujem Vám za pozornosť!

Otázka 1

Aký je zmysel vety "to prevent Internet communication from vulnerability during the election process?"

- zlá vetná konštrukcia
- má znamenať: ochrana posielaných dát a komunikácie

Otázka 2

Aký význam malo písať prácu po anglicky, keď ide o riešenie pripravované špeciálne pre našu univerzitu?

- osobné a slobodné rozhodnutie
- zdroje v angličtine
  - možnosť zachovať ich pôvodnú terminológiu

Otázka 3

Prezentované riešenie nepoužíva ani jednu z kryptografických konštrukcií blind signatures, verifiable anonymous channels, homomorphic encryption, untraceable electronic cash protocol. Nebolo by preto lepšie túto podkapitolu vynechať?

- vhodné ich stručne popísať
  - kapitola 2: prehľad existujúcich riešení
  - techniky sa dajú využiť pri dizajne systémov
  - využívané v niektorých z prezentovaných riešení

Otázka 4

Miestami sú popisy algoritmov nejasné. Napríklad prečo „exactly one record“? Ide len o doslovný prepis zdrojového kódu do anglickej vety, alebo naozaj môže byť zhôd niekedy aj viac? Nebola by lepšia formulácia „ak sa nachádza v tabuľke oprávnených voličov“? Čo znamená „the special 0 character vote“. Je to hlas majúci nula znakov alebo obsahujúci iba jeden znak nuly?

- navrhnutá formulácia je možná
  - volič len raz v správne navrhnutej tabuľke
- špeciálny hlas - nemá sa sčítať
- v implementácii reprezentovaný znakom 0

Otázka 5

Čo znamená „secured USB device“? Akým spôsobom má byť zariadenie zabezpečené a pred čím?

- žiaden obsah pred uložením hlasov
- ochrana zo strany volebnej komiesie
- nič okrem dát, ktoré majú byť prenesené

Otázka 6

Prečo je potrebné šifrovať prihlasovacie meno?

- nie je to potrebné
- kontrola na strane servera
- v implementácii cez premennú prostredia

Otázka 7

Automat reprezentujúci validáciu hlasu akceptuje aj prázdne slovo. Je to tak správne?

- nemá byť akceptované
- predpoklad na neprázdne slovo ako vstup
- nutnosť kontrolovať v inej časti kódu

Otázka 8

Chcete heslo zašifrovať alebo zahešovať? Aký je v tom rozdiel? Prečo chcete šifrovať aj prihlasovacie meno? Prečo v prípade chybného prihlásenia vypíšete iba strohú chybovú správu: „Chyba!“? Prečo cesta k súboru s databázou nie je súčasťou konfiguračného súboru?

- zahešovať s použitím soli
- jednosmernosť hašu
- nie je potreba šifrovať prihlasovacie meno
- strohá hláška je výsledkom nedoladenej implementácie

Otázka 9

Nebolo by lepšie veľkú spoločnú časť zdieľať a neopakovať sa?

- áno, bolo
- zvlášť kód pre rôzne spôsoby prihlasovania
- ostatný kód zdieľať

Otázka 10

Čo znamená komentár "This is to be provided by Cosign, but for now..."?

- pozostatok zo začiatku vytvárania kódu aplikácie
- nepovšimnuté a omylom ponechané v kóde