Zinātnieka pārdomas par i-vēlēšanu drošību

Profesors Jānis Bičevskis
Profesors Andris Ambainis
Latvijas Universitātes
Datorikas fakultāte

Plāns

1. Interneta vēlēšanu apdraudējumi
2. Ārzemju pieredze
3. Interneta vēlēšanu Koncepcija Latvijā

Interneta vēlēšanu soļi

1. (Pirms vēlēšanām) Vēlētājs saņem paroli/kodu, kas ļauj viņam balsot.
2. Lietotājs ievada balsojumu lietojumprogrammā uz sava datora.
3. Balsojums tiek nošifrēts un nosūtīts CVK serverim.
4. (Pēc balsošanas beigām) CVK servera saņemtie balsojumi tiek atšifrēti un saskaitīti.

Kas ir drošs?

Informācijas pārsūtīšana no vēlētāja datora uz CVK serveri (informācija tiek šifrēta ar drošām tehnoloģijām).

Kas nav drošs? (1)

Balsošana uz vēlētāja datora:

- Vēlētājs neredz, vai nošifrētais balsojums, kas tiek nosūtīts uz CVK, sakrīt ar viņa balsojumu.
- Datorvīruss var inficēt/modificēt balsošanas programmu.

Kas nav drošs? (2)

Balsošana uz vēlētāja datora:

- Inficēta programma var nomainīt vēlētāja balsojumu pirms tā nosūtīšanas uz CVK un pielietot pareizos autentifikācijas/šifrēšanas līdzekļus nomainītajam balsojumam.

Kas nav drošs? (3)

Balsu apkopošana uz CVK servera:

- Uzbrukumi no iekšpuses (personāls, kas iesaistīts sistēmas apkalpošanā);
- Uzbraukumi no ārpuses (drošības caurumi).

Sekas - notikušie balsojumi var tikt mainīti;

var tikt pieskaitīti nenotikuši balsojumi.

Ielaušanās var tikt nepamanīta.

ASV pieredze

- 2010, D.C. Digital Vote-by-Mail service.
- Iespēja ārpus ASV esošajiem vēlētājiem balsot caur Internetu.
- 28.09-6.10: sistēmas izmēģinājums.
- Tika plānota izmantošana 2010.g. novembra vēlēšanās.

Pilotprojekta rezultāti

- Uzbrucējs: University of Michigan.
- Uzbrucējs sasniedza gandrīz pilnīgu kontroli pār e-vēlēšanu sistēmu:
  - spēja noteikt katra vēlētāja balsojumu;
  - spēja mainīt vēlētāju balsojumus (ieskaitot balsojumus, kas notikuši pirms ielaušanās brīža);
- Uzbrukums netika pamanīts, līdz uzbrucējs par to pats nepaziņoja.

Tika nolemts sistēmu praksē neizmantot.

ASV pieredzes secinājumi

Publicēts:

Barbara Simons and Douglas W. Jones. Communications of the ACM (2012.gada oktobra numurs)

"Internet Voting in the U.S.“

ASV pieredzes secinājumi

1. Internet voting is fundamentally insecure.
2. Most people do not associate widely publicized computer viruses and worms with Internet voting.
3. Internet voting is being pushed in many countries by vendors, election officials, and well-meaning people who do not understand the risks.

Ārzemju pieredze - Norvēģija

Publicēts: Jordi Barrat i Esteve, Ben Goldsmith and John Turner

International Experience with E-Voting

Norwegian

E-Vote Project, June 2012,pp. 196.

International Foundation for Electoral Systems (since 1987, IFES has worked in over 135 countries).

Ārzemju pieredze - Norvēģija

- The group of Internet voting system users consists of four core countries which have been using Internet voting over the course of several elections/ referenda: Canada, Estonia, France and Switzerland. Estonia is the only country to offer Internet voting to the entire electorate. The remaining seven countries have either just adopted it, are currently piloting Internet voting, have piloted it and not pursued its use, or discontinued its use.

Ārzemju pieredze - Norvēģija

- Finally, it is clear that the field of electronic voting is subject to ongoing technological developments. New functionality is constantly being developed for voting machines, which will continue to raise challenges in the future about the way in which electronic voting is implemented.

Ārzemju pieredze - Igaunija

- I-vēlēšanas kopš 2005. gada.
- Izmantotas 2005, 2007, 2009, 2011. gados.

Helger Lipmaa

Igaunijas vadošais kriptogrāfijas eksperts

«I paper voted. Why? First of all, as a cryptographer, it is my job not to support insecure systems.»

05.03.2011

Barbara Simons

- ASV valdības padomniece e-vēlēšanu jautājumos.

Based on the information I have obtained, I have concluded that the Internet voting system used in Estonia is insecure.

03.09.2011

Problēmas ar Igaunijas e-vēlēšanām (Barbara Simons)

1. There are a number of serious problems, as described by the OSCE/ODIHR report;
2. The voters' privacy (secret ballot) is vulnerable;
3. The voters' computers are vulnerable to election rigging malware;
4. There is an insider threat;
5. The server is vulnerable to attack from anyone/anywhere;
6. The system is not open or transparent;
7. There has been no security evaluation of the system by independent computer security experts.

Problēmas ar Igaunijas e-vēlēšanām (Barbara Simons)

1. There are a number of serious problems, as described by the OSCE/ODIHR report;
2. The voters' privacy (secret ballot) is vulnerable;
3. The voters' computers are vulnerable to election rigging malware;
4. There is an insider threat;
5. The server is vulnerable to attack from anyone/anywhere;
6. The system is not open or transparent;
7. There has been no security evaluation of the system by independent computer security experts.

Situācija Latvijā

1. LVRTC ir izstrādājis interneta vēlēšanu Koncepciju ar zemu drošības līmeni
2. Koncepcija tika analizēta daudzās sanāksmēs, ieskaitot CVK, kur piedalījās arī LATA pārstāvji, formulējot 8 jautājumus, kas skar e-vēlēšanu drošību, lietderību un atbilstību Satversmei.
3. Uz 7 jautājumiem joprojām nav saņemta nekāda atbilde

LU DF vērtējums (1)

Vērtējumu akceptēja - 3 LZA akadēmiķi, 15 profesori, 5 docenti, 11 pētnieki

- Interneta vēlēšanu Koncepcija nesniedz pietiekamu pamatojumu tam, ka nav iespējama i-vēlēšanu rezultātu viltošana; tās priekšrocības, ko piedāvā i-vēlēšanas, neatsver tos milzīgos zaudējumus, kuri iespējami i-vēlēšanu rezultātu viltošanas gadījumā.

LU DF vērtējums (2)

- Starptautiskā pieredze interneta vēlēšanu sistēmu izveidē parāda, ka pasaulē vēl nav izveidota sistēma ar pietiekoši augstu drošības pret viltojumiem līmeni; ASV pieredze pārliecina, ka tuvākajā laikā drošs i-vēlēšanu risinājums nav sagaidāms

Situācija Latvijā

1. Neraugoties uz ekspertu brīdinājumiem, Koncepcija tika iesniegta akceptēšanai valdībā
2. Koncepcijas autori maldina neinformētus cilvēkus un valdību, radot iespaidu, ka Latvija spēj atrisināt pasaulē neatrisinātu interneta vēlēšanu problēmu
3. LU DF darbinieki aicina apturēt šo avantūristisko projektu

Paldies par uzmanību