E-valimiste võimalikud tehnoloogilised platvormid

Tanel Tammet

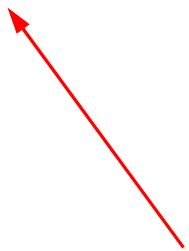
Tallinna Tehnikaülikool

Sisukord

- Mõned ohud ja kuidas neid vähendada
- Kes korraldab ja auditeerib?
- Analoogia tavavalimistega
- E-valimiste tarkvara erisused “tavatarkvarast”
- Minimaalsed vahendid: miks ja kuidas
- Krüptoküsimused
- Auditeerimisküsimused
- Kokkuvõte

Üldpoliitilised ohud

- Valimiste ühetaolisus
- Valimiste osavõtt
- Valimiste hind
- **Legitiimsus ja selle kahtluse alla seadmine**



Ettekande fookus: kuidas tehnoloogiavalikute abil vähendada toimunud e-valimiste kahtluse alla seadmise võimalusi?

Legitiimsus ja kahtlustused

Üksteist võimendavad mõjujõud:

- Paljude valijate paratamatu ebakindlus e-valimiste ususe osas.
- E-valimiste tõttu halvemasse seisu seatud poliitilistel jõududel tekib soov:
  - Toimunud e-valimisi kahtluse alla seada ja tühistada
  - Vältida e-valimiste korraldamist üldse
- Analoogilised soovid tekivad poliitilist olukorda destabiliseerida soovivatel jõududel

Võitmatud ja võidetavad probleemid

Probleem nr 1, mida me ei suudagi päriselt kaotada:

- Häälte ostmise lihtsustumine (e-valija ei ole kabiinis ja teda saab kõrvalt jälgida).

Probleem nr 2, mida saame oluliselt minimeerida:

- Mehhanismi uudsus ja mõistetamatus nii tavavalija kui enamiku spetsialistide jaoks.

Reaalne eesmärk ohtude vähendamisel

Kõiki uusi ohtusid ei ole võimalik kaotada.

Küll aga:

- Toetub valijate arvamus e-valimiste aususe osas
  - Oma intuitsioonile
  - Spetsialistide hinnangutele
  - Poliitikute väidetele
- Mida me peame tegema:
  - Suurendama valijate osakaalu, kel on positiviine intuitsioon
  - Suurendama positiivselt meelestatud spetsialistide osakaalu
  - Siduma võimalikult paljusid poliitilisi jõude auditeerimisega

Tarkvara loomise skeeme

Kuidas valimistarkvara hankida? Variante, enamus neist halvad:

- Ostetakse väljamaalt valmis süsteem
- Tellitakse kogu töö Eestist, mõnelt pangalt
- Riigi juhtimisel tellitakse tükkide kaupa Eestist

Tehnoloogiline platvorm? Variante, enamus neist halvad:

- Mujal valmistehtud süsteem (mistahes platvormil)
- Kohandatud, pangatehnoloogial baseeruv süsteem
- Suletud koodiga (näiteks Microsofti) tehnoloogial baseeruv
- “Standardne” lahtine rakendus: andmebaasimootor, Java vms
- Minimaalne rakendus (vanaaegses stiilis: enamus tehakse ise)

Tarkvara loomine ja audit: kes ja mis

Meil on vaja:

- Vähendada hirmu teadlike pettuste osas
- Positiivselt siduda võimalikult palju spetsialiste
- Positiivselt siduda poliitilisi jõude

Selleks:

- Mitte osta valmistarkvara või uue loomist:
  - välismaalt
  - pankadest vms suurtelt institutsioonidelt
- Mitte osta e-valimiste projekti juhtimist eraettevõtetelt
- Maksta hulgale erakondadele ja MTÜ-dele kinni sõltumatu audit
- Kasulik on kaasata välismaad ja suuri institutsioone auditeerimisse

Mehhanismi mõistmine tavavalija jaoks

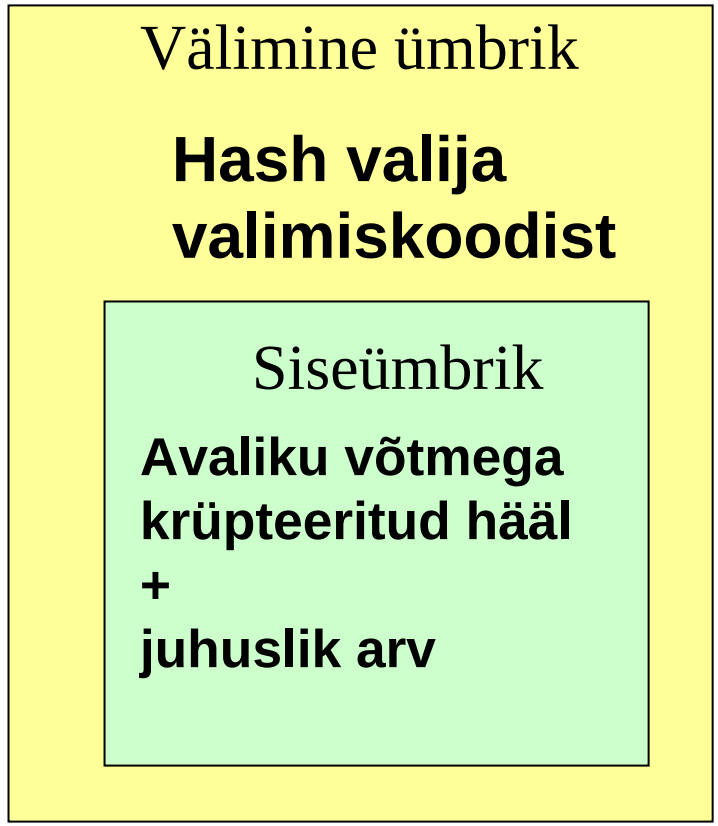
Ainus viis mehhanismi mõistetavaks muuta:

- analoogia mingite “harilike” valimistega
- analoogiat on võimalik saada posti teel valimistega

Seega: realisatsioon peegeldagu posti teel valimisi

- Hääl on “sisemises ümbrikus” ilma valija nimeta
- “Sisemine ümbrik” on nimega, välise ümbriku sees
- Valimisõigusi (nimed!) ja hääli (ilma nimeta!) hoitakse eraldi serverites, eraldi gruppide kontrolli all

Postivalimiste analoogia



“Hariliku tarkvara” loomise põhimõtteid

- **Odav hind**
  - Olemasolevate komponentide ärakasutamine
  - Suurte standardsete baasrakenduste (andmebaas, www-server jne) kasutamine
  - Mugavate kõrgkeelte kasutamine
- **Kerge seostatavus olemasoleva tarkvaraga**
  - Rakendus töötagu võimalikult laialt levinud opsüsteemidel (Windows, Linux, Solaris jms)
  - Realiseeritakse liidestega levinud tehnoloogiate abil (Corba, .net, SOAP, muud XML-liidesed jms)
- **Lihtne edasiarendatavus, portimine jms**
- **Efektne kasutajaliides**

“Hariliku” tarkvara põhimõtted ei sobi!

E-valimiste tarkvara vajadused on pigem vastupidised “hariliku” tarkvara vajadustele

- **Hind** on esmajoones:
  - avalik usaldusväärsus
  - auditeeritavuse odavus
  - **Mitte aga realisatsiooni hind**
- Kerge seostatavus teiste süsteemidega on **halb**, mitte hea!
- Kasutajale **ei ole vaja** müüa suurt funktsionaalsust!

Auditeeritavus ja selle saavutamine

- Võimaldab maksta auditeerimisi erakondadele kinni
- Võimaldab laiendada heatahtlike spetsialistide ringi

Kuidas saavutada:

- 100% lahtine kood: operatsioonisüsteem ja kõik muu
- Mitte kasutada interpretaatoreid (Java, Basic, Python, Perl, PHP jne): väga raske auditeerida
- Mitte kasutada andmebaasimootoreid jms: väga raske auditeerida.
- Minimaalsed teegid, minimaalsed vahendid: mitte kasutada koodijuppe, ilma milleta saaks hakkama

Sobivad tehnoloogiad: konkreetselt

- **Kasutada lihtsamat sorti, stabiilset, vabavara-opsüsteemi:**
  - Kõlbmatu: mitte lahtise koodiga opsüsteem
  - Halvem variant: Linux
  - Parem variant: turvaprioriteediga OpenBSD
- **Programmeerida ainult C keeles**
  - GCC kompilaator on ülilevinud ja lahtise koodiga
  - Saadud assemblerprogrammi saab soovi korral lisaks auditeerida
- **Mitte kasutada andmebaasimootoreid ja suuri servereid**
  - Andmehulk on väike, DB mootoreid pole otseselt vaja
  - Apache jms serverid on liiga suure funktsionaalsusega
- **Mitte kasutada XML-i jms lisakeerukust tekitavat**
- **Kasutada kõige lihtsamaid krüptosüsteeme:**
  - Mitte mõelda ise välja ja programmeerida “uut ja vinget”

Minimiseerimise kaotused ja võidud

- Tarkvara loomine kallineb ca 4-5 korda
  - Aga: tarkvara loomine on eelarvest suhteliselt väike osa: ca 2 milj eelarve 10 miljonist.

- Täielik auditeerimine muutub reaalselt võimalikuks

- Auditeerimist suudetakse kinni maksta või toetada paljudele huvigruppidele:
  - Ühe auditi hind ca 500.000
  - Neli auditit kokku maksab ca 2 milj

- Häälte sõltumatu lugemine suudetakse kinni maksta paljudele huvigruppidele:
  - ühe lugemise hind ca 70.000

Krüptoalgoritmid “posti teel” analoogias

Vähemlevinud ja uuemaid krüptoalgoritme suudab mõista ainult käputäis spetsialiste: kõlbmatu valik!

Piisab:

- Server-brauser vahel https protokoll
- Ühesuunalised hashid valija ning hääle eraldamiseks
- Järjest mitme avaliku võtmega krüpteeritud hääled

Nimetatute eelised:

- Väga levinud
- Olemas “klassikalised” 100% lahtise koodiga teegid

Kokkuvõtteks

- Põhioht on ebakindlus ja surve e-valimiste kahtluse alla seadmiseks.
- Ei ole võimalik kaotada kõiki ohtusid ja probleeme.
- Neid ohte ja probleeme, mida saab minimeerida, tuleb minimeerida.
- Tarkvara osas saame ohte minimeerida, kui:
  - e-valimiste tarkvara loomist ei outsource-ta päriselt välja
  - e-valimiste mehhanismil on posti teel valimiste analoogia
  - tarkvara on 100% lahtise koodiga
  - tarkvara luuakse minimaalsete vahenditega
  - sõltumatu auditeerimine makstakse kinni võimalikult paljudele huvigruppidele