E-hääletuse lühiajalugu

- Lähteuuringud 2001, protokoll 2003, valimised 2005
- Protseduuriline vs krüptograafiline kontroll
  - 2013 valija isikliku hääle kontroll QR-koodiga
  - 2015 „Vaadeldamatu e-hääletus pole usaldusväärne”
  - 2017 kuulutas RVT läbinisti kontrollitavaks
- Valimiskaebus 2019: dekrüptimine enne miksimist
- Kingo komisjon: õiguslikult määratleda kontrollitavus
- Viis nõudmist 2023: nõuame vaadeldavat e-hääletust!

Ausad Valimised  Fair Elections Estonia

OSCE/ODIHR 2023. aasta vaatlusraport

1) „Nagu eelnevalt soovitatud, peaksid valimiste korraldajad kaaluma meetodeid, kuidas saavutada läbiv (*end-to-end*) kontrollitavus. Praeguste kontrollitavuse mehhanismide parandamiseks peaksid valimiste korraldajad kõrvaldama puudused individuaalses kontrollitavuses ja tagama, et kõik e-hääletamise tulemuste kindlaksmääramise kriitilise tähtsusega etapid oleksid auditeeritavad."

2) „Piisavaid vahendeid omav siseringi kuuluv isik võib, kui ta suudab seda teha märkamatult, kontrollida, millised hääled eemaldatakse, ja seega osaliselt mõjutada tulemusi."

On the Auditability of the Estonian IVXV System and an Attack on Individual Verifiability

Anggrio Sutopo, Thomas Haines, Peter Rønne

Since the project only manages to fulfil one of the nine standards, minimal restrictions on disclosure, we foresee, inline with prior work, that the system likely has vulnerabilities. This conjecture is supported by the vulnerability discussed.

3.6 Why wasn't this already noted?

The vulnerability is straightforward which makes it more concerning. The fact that is hasn't been noticed until now we put down to the fact examinations of the IVXV system, [illegible]

In the next sectio
the code of the IV

Our work highlights the significant deficiencies in the source code of the IVXV system which has been made available. These deficiencies increase the effort of examiners to audit the system and seem to have been fairly effective in preventing even simple vulnerabilities from being discovered. As an example of this, we point to the vulnerability in verifiability which should have been apparent even at the specification level. We make the following recommendations:

Ohu nimetus: Mõned e-hääletamise etapid võivad jääda auditeerimata/vaatlemata, sest tänane protokoll seda ei võimalda

Ohusündmuse lühikirjeldus

Internetihääletamise protsesside ja protokolli keerukuse ning väliste osapoolte (usaldusteenuste pakkujad, sisulevivõrgud jt tootmis- ja tarneahela osapooled) olemasolu tõttu pole võimalik kõiki valimiste etappe auditeerida. Vaatleme järgmiseid näiteid, mis probleemi illustreerivad

Ohu nimetus: Mõned valimiste etapid võivad jääda auditeerimata/vaatlemata, kuigi see oleks võimalik

Ohusündmuse lühikirjeldus

Auditeerimisjuhend (e-hääletamise käsiraamat ja githubis olev juhend) ei kata kõiki häälte töötlemise etappe, mistõttu on e-hääletamist auditeerival audiitoril palju valikuvabadust. Näiteks ei ole audiitoril kohustust kontrollida võtme loomiseks ega sedelite töötlemiseks kasutatud tarkvara terviklust ja autentsust. Vaatlejatel ei ole lubatud niisuguseid kontrolle teostada. Kuna audiitorijuhend ei kata kõiki töötlemise samme, siis ei ole kindlust, et kõik etapid saavad auditeeritud. Lisakontrollide teostamine sõltub audiitori põhjalikkusest, e-hääletamise süsteemi ehituse mõistmisest ning audiitori tehnilistest oskustest.

KPMG 2021. aasta e-valimiste auditi lõpparuandes nõuti mainitud

olmanda osapoole (SK ID Solutions)
imiskinnituste korrektset säilitamist
oimalik kontrollida.
inevaid andmekeskuseid ja nende
a kontroll pole valimiste audiitorile

ollimiseks peaks audiitor olema
ndades paberhääletamisest osavõttu,
mes rollis (audiitor ja valimiste

mille alla võib käia hulk detailsemaid
met valimistulemuse vastu, kuid
estumiseks.

ese, info, sidekanal,
ne urn

Sõnum on kohale jõudnud

- Sotopo/Haines/Rønne 2023: viga individuaalse kontrollitavuse krüptograafias, tarkvara kvaliteet 1/9, oletatavasti samasuguseid vigu veelgi
- Treier/Düüna 2024: siserünne enne 2024 triviaalne
- TA küberturvalisuse komisjon 2024: (5) ei kasutata olemaolevaid kontrolle piisavalt ja (4) protokoll kõike vajalikku kontrollida ei võimaldagi

Ausad Valimised  Fair Elections Estonia

Saksamaa konstitutsioonikohus 2009:
Valimiste avalikkuse põhimõte

1) Valimiste avalikkusse põhimõte PS artikli 38 alusel koostoimes artikli 20 lõigetega 1 ja 2 nõuab, et valimiste kõik olulised sammud oleks avalikkuse poolt kontrollitavad, välja arvatud juhul, kui muud põhiseaduslikud nõuded õigustavad erandit.

2) Elektrooniliste hääletusmasinate kasutamisel peavad valmiste läbiviimise ja tulemuste kindlakstegemise olulised sammud olema kodanikele usaldusväärselt ja eriteadmisteta kontrollitavad.

OSCE/ODIHR 2019. aasta raport

„ODIHR EET poolt läbiviidud tehniliste ja protseduuriliste raamistike analüüs osutab, et siseründaja, kellel on võimalik ligi pääseda digitaalsetele hääletussedelitele, võiks murda iga valija hääle salajasuse tema poolt veebis avaldatud QR-koodi abil — ja seda isegi pärast koodi kehtivuse lõppu. See on vastuolus riiklike seaduste ja rahvusvaheliste standarditega, mis puudutavad hääle salajasust.”

** CM/Rec(2017)5 e-hääletamise standardite kohta sätestab, et e-hääletamine peab olema korraldatud nii, et häälte salajasus on tagatud kogu valimisprotsessi kõikides etappides.*

UUDIS

Ajakirjanikel oli teoreetiline võimalus president Alar Karise e-hääle salajasuse murdmiseks

Valimisteenistus ei hakka uurima, kas keegi kõrvaline isik tutvus presidendi häälega

Ronald Liive

03.03.2023 kell 14:25

President Alar Karis andis Riigikogu valimistel e-hääle eile Kiidjärve raamatukogus. Foto: Vabariigi presidendi kantselei

Riigikohus 2005 kaasuses 3-4-1-13-05
607 SE põhiseaduslikkusest

30) Valija, keda on elektroonilise hääletamise käigus ebaseaduslikult mõjutatud või jälgitud, saab taastada valimiste vabaduse ja hääletamise salajasuse, hääletades mõjutustest vabanenult uuesti elektrooniliselt või valimissedeliga.

14) Vabariigi President ei vaidlusta ja kolleegium käesolevas asjas ei käsitle elektroonilise hääletamise üldist kooskõla Eesti Vabariigi põhiseadusega.

6. Ei saa veenduda arvutites olevas tarkvaras
5. Pole tagatud valimissaladus (2-3x tähenduses)
4. Praktiline vaatlemine/kontroll pole tagatud
3. Sammud pole sõltumatult tervikuna kontrollitavad
2. Puudub kaebeõigus üldistes huvides
1. ~~Reguleeritud RVT/VVK aktide, mitte seadustega~~
    1) Võeti vastu kiirustades ja konsensuseta
    2) Puudub e-hääle õiguslik määratlus
    3) Vaatlemise õiguslik tähendus määratlemata
    4) Salajasus on määratletud üldsõnaliselt

2024: Kas Eesti internetihääletuse süsteemi jätkuv kasutamine on õigustatud ja turvaline ka siis, kui eespool kirjeldatud vastuolud ei ole asjakohaselt lahendatud?

2007: Kui internetihääletust puudutavatele tõsistele probleemidele ei leita tõhusat lahendust, tuleks tõsiselt kaaluda, kas see peaks olema laialdaselt kättesaadav hääletusmeetod, või alternatiivselt, kas peaks seda kasutatama piiratud alustel või üldse mitte kasutama.

2025: Mis tingimustel võiks e-hääletus olla lubatav?