

Austraalia teadlased lammutasid Eesti e-valimiste koodi algosadeks: mida leiti?

2 tundi tagasi - 28.10.2026 Autor: [AM](#)

Mis juhtub siis, kui teisel pool maakera istuvad tippteadlased võtavad meie rahvusliku uhkuse ehk e-valimiste süsteemi ette, harutavad selle avaliku lähtekoodi rida-realt lahti ning hakkavad sealt teadlikult nõrku kohti otsima? Just seda tegidki Austraalia Rahvusülikooli (ANU) uurijad Tingfeng Yu ja Thomas Haines, kelle värske ja mahukas teadustöö toob päevavalgele kümme seni teadmata teoreetilist haavatavust.

Enne kui haarata paaniliselt fooliummütsi või paberhääletuse järele, tasub siiski sügavalt sisse hingata. Kuigi teadustöö pealkiri ja leitud vigade arv võivad esmapilgul kõlada ehmatavalt, kinnitavad nii ookeanitagused uurijad kui ka meie oma Riigi valimisteenistus (RVT) ja Riigi Infosüsteemi Amet (RIA): ühtegi neist nõrkustest pole Eesti valimistel kunagi ära kasutatud. Veelgi enam, selline "valge mütsi" häkkerite ja teadlaste torkimine ongi täpselt see põhjus, miks Eesti oma e-valimiste lähtekoodi avalikuna hoiab.

E-hääletus kui keeruline Šveitsi kellavärk

Austraalia teadlaste peamine etteheide Eesti e-hääletuse süsteemile (mille tehniline nimi on IVXV ja mis on sellisel kujul kasutusel 2017. aastast) ei seisne selles, et süsteem oleks läbinisti katkine, vaid selles, et seda on väljastpoolt raske kontrollida. Kuigi kood ja üldine dokumentatsioon on GitHubis kõigile vabalt saadaval, puudub süsteemil üks täpne, matemaatiliselt formaliseeritud "emajuhend".

Olukorda võib võrrelda sellega, kui sulle antakse kätte tuhandest hammasrattast koosnev ülikeeruline Šveitsi käekell ja karbitäis varuosi, kuid täpset joonist selle kohta, kuidas iga pisimgi vedru ekstreemses olukorras käituma peab, pole. Nii pididki Yu ja Haines tegema ära suure pöördprojekteerimise töö. Nad ehitasid avaliku koodi ja konfiguratsioonifailide põhjal üles tervikliku, 181-leheküljelise mudeli, mis katab kõik valimiste etapid: seadistamise, hääletamise, häälte kokkulugemise ja auditeerimise.

Teadlased märgivad oma töös otsekoheselt: "Eesti IVXV süsteem on üks maailma pikima ajalooga ja suurima mahuga internetihääletuse rakendusi, kuid sellel puudub teostatud protokoll täpne avalik spetsifikatsioon või turvaväited, mis on teinud selle sõltumatu auditeerimise keeruliseks."

Samuti lisavad nad oma leidude kohta: "Me avastame mitmeid seni teadmata haavatavusi – mis hõlmavad hääletussedeli salajasust, individuaalset kontrollitavust ja universaalset kontrollitavust, millest paljud tulenevad ebajärjekindlast valideerimisloogikast komponentide vahel, kodeerimiserinevustest ja kontrollimata krüptograafilistest parameetritest – ning valideerime valitud leiud kontseptsioonitõestuse (PoC) testidega, mis panevad proovile tegeliku rakenduse."

Kümme teoreetilist rünnet: pahavarast süleris kuni ajatemplite trikitamiseni

Kui teadlased olid oma mudeli valmis saanud ja seda Šveitsi (Swiss Post) ning Prantsuse päritolu (Belenios) e-valimiste süsteemidega võrrelnud, leidsid nad kümme uut teoreetilist ründevektorit ning neliteist väiksemat kooditaseme tähelepanekut. RVT vaatas need leiud koos arenduspartneriga hoolikalt läbi ning selgitas, et kriitilisi turvanõrkusi nende seas ei ole – kõik kümme stsenaariumi eeldavad väga spetsiifilisi eeltingimusi.

Laias laastus jagunevad teadlaste leitud "augud" järgmiselt:

- **Nakatunud süler või nutiseade** (leiud IV-V1, IV-V4, IV-V5, IV-V6): pea pooled leidudest eeldavad, et ründaja on saanud täieliku kontrolli sinu arvuti (valijarakenduse) või allkirjastamisseadme üle. Näiteks kirjeldavad teadlased olukorda, kus pahavara laseb sul küll hääle ära anda ja näitab nutitelefonil kontrolläpis, et kõik on korras, kuid saadab taustal teele hoopis varem salvestatud häälekonteineri või kasutab ära seda, kuidas erinevad süsteemi osad tõlgendavad negatiivseid arve krüptogrammis. Selle tulemusel visatakse sinu viimane hääl hiljem lugemisel kui "vigane" lihtsalt kõrvale.
- **Kuri ajatempliteenuse pakkuja** (leid IV-V3): Eesti e-valimistel saad oma häält muuta nii mitu korda, kui soovid – arvesse läheb vaid viimasena antud hääl. Teadlased tõid välja, et kui väline registreerimisteenuse pakkuja (kes väljastab häälele ajatempli) oleks pahatahtlik, saaks ta teoreetiliselt 60-sekundilise akna sees sinu hääle kellaagu nihutada nii, et peale jääb hoopis sinu varasem, mitte viimane hääl. RVT rõhutab siinkohal, et seda teenust pakub SK ID Solutions, mis vastab maailma rangeimatele eIDAS ja

ISO turvastandarditele, kuid sellegipoolest võetakse ajatemplite rangem kontroll töösse.

- **Kontrolläpi pimesi usaldamine** (leid IV-V2): uurijad leidsid, et kui hääle vastuvõtja (kogumisteenus) rikub meelega ära hääle ajatempli räsialgoritmi klappivuse, siis sinu nutitelefoni kontrolläpp seda viga ei märka ja ütleb, et häälel on korras. Hiljem, kui hääli kokku loetakse, praagib keskseade selle hääle aga välja. See on üks neist praktilistest leidudest, mille RVT lubas kohe järgmisteks valimisteks ära parandada, täiendades kontrolläpi loogikat.
- **Häälte salajasus ja "mitu küsimust"** (leiud P-V1, P-V2): teadlased avastasid koodist ohtliku vea (P-V2), kus mitme küsimusega valimiste puhul kasutab süsteem sama juhuarvu (*randomness*), mis võimaldaks krüptogramme kõrvutades valija eelistused lahti muukida. Õnneks on siin lihtne konks: Eesti seadused ei luba nagunii korraldada valimisi, kus ühel sedelil on korraga mitu küsimust, seega pole seda funktsiooni kunagi kasutatud. RVT kaalub nüüd selle "uinunud" koodijupi täielikku eemaldamist. Teine krüptograafiline leid puudutas vanemat algoritmi loogikat, mille Eesti vahetas uue vastu välja juba 2025. aastal.

Kas kontrolläpp peaks teadma, kes sa oled?

Üks põnevamaid filosoofilisi ja tehnilisi vaidlusi Austraalia teadlaste ja Eesti e-valimiste arhitektide vahel tekkis leiu IV-V4 ümber. Teadlased tõid välja niinimetatud identiteedi asendamise ründe: kui sinu süler on pahavaraga nakatunud, võib see sind petta kontrollima hoopis kellegi teise (näiteks ründaja kaasosalise) antud häält, kus on kirjas sinuga sama kandidaat. Kuna kontrolläpp näitab sulle õiget kandidaadi nime, jääd sa rahule, kuid tegelikult sinu häält süsteemis polegi.

Lahendusena pakkusid austraallased välja, et nutitelefoni kontrolläpp võiks olla isikustatud – näiteks nõuda sisselogimist või isikukoodi kinnitamist. RVT lükkas selle soovitusel aga kindlalt tagasi, viidates Eesti e-hääletuse ühele alustalale. Kui muuta kontrolläpp isikustatuks, kaoks ära seadmete sõltumatus. Praegune loogika on ehitatud nii, et nutiseade, millega sa arvutiekraanilt QR-koodi skannid, on täiesti "tumm" ja anonüümne vaatleja. Kui pahavara või ründaja teaks täpselt, kes kontrolläppi kasutab, tekiks oht, et ka kontrollimise protsessi ennast hakatakse sihitult manipuleerima.

Siin kehtib vana hea küberturvalisuse kuldreegel: oma seadmes tuleb kasutada ametlikku tarkvara ja hoida viirusetõrje ajakohasena.

Parem karta kui kahetseda: pilk 2027. aasta Riigikogu valimistele

Mida see teadustöö siis kokkuvõttes näitab? Esiteks seda, et ükski tarkvara pole kunagi lõplikult "valmis". Isegi 20 aastat lihvitud süsteemis tekib komponentide uuendamisel ebakõlasid – näiteks kontrollib üks moodul andmeid veidi teisiti kui teine.

Yu ja Haines kasutasid teadustöös muudetud koodiga lokaalseid mudeleid ega rünnanud kordagi päris valimiste servereid. Oma avastustest andsid nad Eesti poolele teada juba alates 2025. aasta sügisest ja 2026. aasta kevadest, jättes piisavalt aega süsteemi lappimiseks.

Teadlased ise võtavad oma töö eetika ja mõju kokku nii:

"See töö raporteerib haavatavustest IVXV süsteemi protokollis; kas neid oleks saanud kasutusel olevas süsteemis ära kasutada, ei ole võimalik meile kättesaadava teabe põhjal hinnata. Meil ei ole põhjust arvata, et neid oleks ära kasutatud. Lisaks ei kasutata meie analüüsitud versiooni tulevastel valimistel."

Uurijate luubi all oli 2025. aasta kohalike omavalitsuste valimistel kasutatud tarkvaraversioon (KOV2025). Praegu käib RVT-s ja arenduspartnerite juures töö uue versiooni kallal, mis läheb käiku 2027. aasta märtsis toimuvatel Riigikogu valimistel.

- [Uudised](#)
- [Tarkvara](#)
- [Turvalisus](#)

Pilt

Algorithm 55: DecryptBallotbox - [Link to Code](#)

Input:

eid : String. Election ID.
 (t, n) : Tuple<Int, Int>. Threshold Decryption setting: t : threshold, n : number of shares
 P_{eg} : ElGamalParameters
 BB_{mixed} : AnonBallotbox. Mixed, anonymised ballotbox
 sk : Int. Reconstructed decryption key
 $checkDecodable$: Bool: indicates whether validation on ballot ciphertext needs to be performed.
 $withProof$: Bool: indicates whether outputting decryption proof of valid votes.

Output:

BB_{dec} : DecryptedBallotbox. Decrypted ballotbox

Operation:

```

1   $pk \leftarrow (P_{eg}.g)^{sk}$ 
2   $BB_{dec} \leftarrow DecryptedBallotbox(eid, \emptyset)$ 
3  foreach  $(d, P) \in BB_{mixed}.M$  do
4      foreach  $(p, Q) \in P$  do
5          foreach  $(qKey, B) \in Q$  do
6               $BB_{dec}.M[d][p].put(qKey, [])$ 
7              foreach  $b : Byte[] \in B$  do
8                   $ok \leftarrow true$ 
9                   $v : DecryptedVote \leftarrow DecryptedVote(d, p, qKey, b, null)$ 
10                 if  $checkDecodable$  then
11                      $ok \leftarrow isValidCiphertextPA(P_{eg}, pk, b)$ 
12                 if  $ok$  then
13                      $dp \leftarrow ElGamalDecrypt(sk, b, withProof)$ 
14                     if  $dp \neq \perp$  then
15                          $v.dp \leftarrow dp$ 
16                      $BB_{dec}.M[d][p][qKey].append(v)$ 
17  return  $BB_{dec}$ 

```