EESTI TEADUSTE AKADEEMIA

Teaduste akadeemia küberturvalisuse komisjoni koosoleku protokoll 7. jaanuaril 2025. aastal

Tartu Ülikooli raamatukogus ja Zoomi keskkonnas

Algus kell 10.30
Lõpp kell 15.00

Juhatas akadeemik Dan Bogdanov

Osalesid: Kati Ambo-Vaher, Arne Koitmäe, Alo Einla, Kristjan Krips, Ivo Kubjas, Priit Parmakson, Guido Pääsuke, Teet Raidma, Tanel Tammet, Jan Villemson, Priit Vinkel, Liisa Past Indrek Leesi, külalisena Sven Heiberg SCCEIV-st.
Puuduvad akadeemik Anu Realo ja Ahto Truu seoses tööülesannetega.

Protokollis: Ülle Sirk

1. Mis tehtud, mis teoksil? Valimiste tehnoloogia ja õiguse alaste uudiste jagamine

Arutelus osalesid kõik istungil osalejad. Külalisena liitus Sven Heiberg SCCEIV-st, et arutada kohtumisi nutiseadmete operatsioonisüsteemide tootjatega.

a) Sven Heiberg andis ülevaate nutiseadmete operatsioonisüsteemide tootjatega (Apple, Google) tehtavast koostööst, et leida parim võimalus neil seadmetel valijarakenduse levitamiseks. Toimunud on kõnesid ning kaalumisel on mitu varianti. Eelistatakse variante, mis on kooskõlas Eesti seadusandlusega ning lihtsustavad audiitori tööd.
b) Jan Villemson ja Liisa Past diskuteerivad kvantarvuti ohtude ja tuleviku küsimustes. Akadeemik Bogdanov nendib, et kvantarvutiga seoses räägitakse reaalsest ohust, millega aga kaasnevad nii ootused kui hirmud. Üleminek kvantarvuti vastu kaitsvale postkvant-krüptograafiale on kindlasti mõistlik seal, kus krüptoskeemid on saavutanud küpsuse ja on standarditud. Seal on postkvant-krüptograafiale üleminek minimaalsete kuludega juba täna. Keerulisemad süsteemid nagu digitaalne identiteet ja internetivalimised vajavad veel teadustööd ja tehnoloogiaarendust. Internetivalimiste kontekstis – kui kunagi ehitatakse täna standardset krüptograafiat murdev kvantarvuti, siis saaks kellegi poolt salvestatud e-hääli lahti krüpteerida ja valimissaladust murda.
c) Liisa Pastile tundub see väljavaade veidi hirmu õhutamisena ning ta märgib ära, et Eestis e-hääli ei arhiveerita ja need hävitatakse. Akadeemik Bogdanov täpsustab, et ametlikult tõesti massiliselt ei salvestada, kuid kui kellelgi õnnestub koguda ka vähene kogus hääli, on see ohukoht. Fakt on, et täna ei saa me enam vähendada ohte postkvant-krüptograafiata antud e-häältele, aga me saame oluliselt vähendada potentsiaalselt rünnatavate häälte hulka kaugemas tulevikus.

d) Teet Raidma hinnangul tuleks lisada lisakaitsemeetmetena audiitori kontroll e-häälte krüptogrammide juurdepääsu üle. Järgnes arutelu, kas audiitori ülesannete hulka häälte kopeerimise vältimise lisamine on mõistlike ressurssidega saavutatav.

Informatsioon võeti teadmiseks.

2. Arutelu TA küberturvalisuse komisjoni memost VVK-le

Arutelus osalesid kõik istungil osalejad.

a) VVK on kaalumas nutiseadmetega internetivalimiste poolt- ja vastuargumente ning kaaluks teiste seas ka TA komisjoni seisukohti ja hinnanguid ohtudele.

Otsustati, et TA küberturvalisuse komisjon viimistleb komisjonis hinnatud nutiseadmetel valimiste ohtude kirjeldused ning valmistab kaaskirja. Pärast kooskõlastamist komisjoni sees edastatakse materjal VVK-le.

3. Riskide hindamise metoodikast

Avaettekande pidas komisjoni liige Jan Villemson. Järgnenud arutelus osalesid kõik istungil osalejad.

a) Jan Villemson esitas argumendid, miks komisjon peaks muutma oma avaldamisele minevate ohtude valiku metoodikat. Murekohaks on seni kasutusel olnud madal-keskmine-kõrge-väga kõrge lävendid, mis on aritmeetiliselt kunstlikud.
b) Jan Villemson arvutas välja 2023/2024 hinnatud ohtudele hinnete põhjal statistilised usaldusvahemikud ja selle põhjal oleks võinud vabalt avaldada veel mõned ohud, mis praegu jäid lävendi alla. Ning näiteks nutiseadmete rakenduste auditeeritavuse oht oleks võib-olla pidanud saama ohuklassiks „kõrge“.
c) Akadeemik Bogdanov ning komisjoni liige Jan Villemson olid kohtunud sellel teemal ka akadeemik Krista Fischeriga, kellega arutasid komisjoni hääletusmetoodika matemaatilisi aluseid. Akad Fischer matemaatika asjatundjana kinnitas, et statistiliste mõõdikute (keskmiste) korrutamisel võib viga võimenduda ja väga terav lävend ei ole võib-olla otstarbekas. Arutati ka teisi statistilisi funktsioone, kuid üldine probleem jääb samaks sõltumata sellest, kas keskmised on aritmeetilised või geomeetrilised.
d) Järgnes arutelu, kus toodi välja nii metoodika plusskülgi (kõik komisjoni liikmed peavad ohu läbi töötama enda jaoks ning aktiivselt kaasa mõtlema, tegemist on standardse ja palju kasutatud metoodikaga) kui ka miinuskülgi (kunstlik lävend, madala võimalikkuse kuid ülikõrge mõjuga ohte peaks saama avaldada riskihalduse parandamiseks).
e) Akadeemik Bogdanov oli istungiks ette valmistanud mitmed uued hinnangute statistilised analüüsid, mille põhjal tegi ta ettepaneku, et edaspidi komisjon ei vali avalikustamiseks ohte rangelt lävendi järgi vaid lisab avalikustamisse täiendavaid ohte, mille avalikku käsitlemist komisjon peab vajalikuks.

Otsustati küsimuse juurde tulla tagasi kevadel kui asutakse avaldama järgmist versiooni riskianalüüsist.

4. Ohtude hindamine

Ohtude hindamises osalesid kõik istungil osalejad.

a) Komisjon hindas ohtu „Nutiseadmete operatsioonisüsteemide paljusus tõstab koormust valimiste kasutajatoele".
b) Komisjon hindas ohtu „Piisavalt võimas kvantarvuti murrab täna kasutatava avaliku võtme krüptograafia".
c) Komisjon hindas ohtu „Välisriikidest posti teel hääletades on oht hääletamise salajasusele ja käideldavusele".
d) Komisjon käsitles ohtu „Valijarakenduse lähtekoodi mitteavalikkus segab auditit" ning arutelu järel otsustati see ümber kirjutada kaheks ohuks, millest üks käsitleb avalikustamise ohtusid ja teine mitteavalikustamise ohtusid ning siis hinnata neid sõltumatult.

Ohtudele anti hinnangud (välja arvatud valijarakenduse lähtekoodi avatuse oht, mis saadeti uuele toimetamisringile).

Järgmise koosoleku aeg

Järgmine koosolek toimub 11. veebruaril 2025 Tartu Ülikooli raamatukogus