EESTI TEADUSTE AKADEEMIA
KÜBERTURVALISUSE KOMISJON

Küberturvalisuse komisjoni töökoosoleku

protokoll nr. 2

Tallinnas, 13.09.2023
Toimumise aeg kell 11.00-15.00
Koosolekul on võimalus osaleda ka Zoomi vahendusel

Osalevad: akadeemik Dan Bogdanov (komisjoni esimees), Teet Raidma, akadeemik Tarmo Uustalu, Ivo Kubjas Zoomis, Ahto Truu, Jan Willemson, Alo Einla, Kristjan Krips, Arne Koitmäe, Mihkel Solvak, vaatlejaliige Indrek Leesi Zoomis.
Puuduvad: Priit Vinkel, Liisa Past.

PÄEVAKORD

1) 11:00-11:45 Eelmisel istungil esitletud turvamudeli ja näidisohtude tagasiside. Kõik komisjoni liikmed annavad ülevaate enda tehtud analüüsidest (kodutöö) ja üldise mudeli sobilikkusest.
2) 11:45-12:30 Arutelu komisjoni teadlaste koostatava ohtude kataloogi võimalikkuse üle. Millised on tingimused, et TA komisjon võiks ühe oma väljundina toota sellist ohtude kataloogi, mis oleks avalikustatav? Kus võiks seda avalikustada ja kuidas arendada?
3) 13:15-14:15 Arutelu internetihääletuse süsteemi tooteomaniku vastutuse üle. Kas meil on konsensus selles osas, kes on internetihääletuse tooteomanik infotehnoloogilise ja ühiskondliku teenuse arenduse mõttes? Kui konsensuse leiame, siis kuidas võiks efektiivselt olla korraldatud tooteomaniku suhtlus avalikkusega (sh TA komisjoniga) süsteemi arenduseks või uurimiseks? Näiteks, milline oleks efektiivne ja turvaeesmärke tagav protsess protokollile ettepanekute tegemiseks ja nende läbikaalumiseks?
4) 14:15-15:00 Oktoobrikuise TA komisjoni konverentsi päevakavast. Komisjoni juht esitab oktoobri komisjoni päevakava mustandi ning arutame selle sobivust.

PROTOKOLL

1. Üldised teadaanded
    a. Riigi valimisteenistus (RVT) esitas eelmise istungi järel ettepaneku, et komisjon kaasaks Indrek Leesi RVTst vaatlejaliikmena. Komisjoni esimees nõustus ettepanekuga.
    b. Elektroonilise hääletamise regulatsiooni muudatusi ei ole TA küberturvalisuse komisjonile otse kommenteerimiseks saadetud. Seega komisjon ka eraldi osapoolena vastuseid ei esita. RVT esindaja Arne Koitmäe innustas komisjoni liikmeid siiski eelnõuga avalikus infosüsteemis tutvuma ning tagasisidet saatma, kas või RVT-le otse.
    c. Komisjon võttis ka teadmiseks, et Teaduste Akadeemia küberturvalisuse komisjon on saanud tähelepanu Riigikogus ning rahvasaadikute esitatud arupärimises.
2. Valimiste turvaohtude modelleerimise kodutööde ülevaatus
    a. Kodutööna oli komisjoni esimees palunud kirjeldada mõnda valimistega seotud ohtu lähtudes eelmisel istungil esitatud ohumudelist ning Kristjan Kripsi ja Jan Villemsoni ettevalmistatud näidetest.
    b. Enda töö olid esitanud komisjoni liikmed Bogdanov, Einla, Kubjas ja Vinkel.
    c. Järgnes arutelu selle üle, milline on mõistlik detailsusaste, millistes olukordades tasub kasutada suuremat detailsusastet ja kas see sobib nii tehniliste kui mainerünnete modelleerimiseks.
    d. Liikmed nõustusid, et ohuanalüüse kindla struktuuri järgi läbi tehes tekivad seosed ning ohu parem mõistmine. Üksikasjalikult vaadeldi Ivo Kubjase tehtud ohuanalüüsi, mis oli ääretult detailne, kuid samas ei kirjeldanud kuigi kõrge tõenäosusega ohtu. Selle pealt tõstetus arutelu, kuidas läheneda selliste riistvara- ja tarkvarakomponentide, mida ei ole Eestis arendatud, vigu ning arutleti ka sõltumatute valimis- ja verifitseerimissüsteemide teostuste häid ja halbu külgi. Arutleti, mida teha, kui peaks esinema oht, mille puhul leevendusmeetmed ei ole võimalikud. Konkreetsete järeldusteni ei jõutud.
    e. Teet Raidma juhtis arutelu teemal, millised peaksid olema mõjuanalüüsi jaoks vajalikud mõõdikud ning lubas koos Indrek Leesiga teha ettepaneku, tuginedes RVT praegusele mõõdikute ja skaalade süsteemile.
3. Avaliku ohtude kataloogi võimalikkusest

a. Komisjoni esimees esitas ettepaneku, et Eestis võiks olla kriitilistele e-riigi süsteemidele hallata avalikku ohtude kataloogi. Selle eesmärgid oleks pakkuda heal tasemel materjale riigile oluliste teenuste (mitte vaid valimiste – tulevikus ka näiteks tehisintellekti, identiteedilahenduste vms) usaldusväärsuse ja turvalisuse hindamiseks, toetada avaliku diskussiooni ning uute turvaohtude ilmnemisel võimaldaks hinnata uuesti varasemalt madalaks ohuks hinnatud ohte.
b. Praktiliselt saaks TA komisjon välja töötada kataloogi struktuuri ning selle üle anda näiteks Riigi Infosüsteemi Ametile avalikuks majutamiseks (koodivaramu.eesti.ee hoidlas). Kataloogis oleks valimiste kohta käiva omanik siis kas RVT või VVK.
c. Seejärel saaksid teadusrühmad ja riigi turvapartnerid oma turvaanalüüse teha etteantud standardi järgi ning tulemused vaadataks üle vastava teenuse omaniku ning selle turvatiimi poolt ning siis avalikustataks.
d. Järgnes arutelu selle üle, millistel tingimustel selline kataloog võimalik oleks ja kuidas korraldada avalikustamist. Komisjoni liikmed esitasid mitmeid poolt- ja vastuargumente, viidates nii Šveitsi heale kogemusele avalikustamisega kui ka võimalikule ohule, et kaebuste maht ning menetlemise aega valimiste järgselt pikeneb veelgi. Viimasele argumendile esitati ka vastuargument, et kvaliteetne ohtude kataloogi võimaldab tehnilistele kaebustele efektiivsemalt vastata.
e. Arne Koitmäe nentis, et täna ei ole VVK-l ja RVT-l piisavalt tööjõudu, et sellise ohtude kataloogi avalikustamise tööd ja haldamist ette võtta.
f. Komisjon sõnastas ettepaneku, et RVT või VVK peaks saama lisajõudu, et sellist avalikustatavat ohtude kataloogi hallata.
g. Dan Bogdanov ja Alo Einla pöörduvad RIA poole, et uurida, kas koodivaramu.eesti.ee sobiks kataloogi majutajaks.

4. Arutelu valimiste teenuse omaniku rolli üle
    a. VVK, RVT ja RIA esindajad tegid ülevaate tänasest valimiste ja selle tehnoloogiate juhtimisest. Komisjoni liikmed küsisid selgitavaid küsimusi ning tekkis ühine arusaam olukorra seisust.
    b. Jan Villemson selgitas, et paigas peaks olema selge läbipaistev protsess, mille kaudu riik teeb tulevikku vaatavaid arendusi, sh protokollide osas. Perspektiivis vajame näiteks kvantarvutite vastu kindlast internetivalimiste

süsteemi. Täna tehakse sellel teemal Eestis teadustööd, aga pole selge, kuidas võiks näiteks postkvantkrüptograafia, otsast otsani verifitseerituvus ja teised protokollimuudatused formaalselt ametliku internetivalimiste protokolli osaks saada. Lisaks tuleks teatud suuremate arenduste puhul (nt otsast-otsani verifitseeritavus) kaaluda ka rahvusvahelisi hankeid. Kuid ka selleks peab Eesti riigis tellija olema tehniliselt võimeline seda korraldama ning panema välja töörühma, kes suudab pakkumiste sobivust tehniliselt hinnata.

   c. Arne Koitmäe toonitab veelkord, et üliioluline on VVK ja RVT ressursi küsimus. Selle taha jäävad mitmed sellised algatused.

5. Teaduste Akadeemia küberturvalisuse komisjoni konverentsist
   a. Konverents tööpealkirjaga „Usaldusest ja usaldusväärsusest“ toimub Tallinnas akadeemia majas 17. oktoobril 10:00-17:00. Konverentsi eesmärk on tutvustada komisjoni tööd ja koguda tagasisidet ja ettepanekuid.
   b. Päevakava on kolme peamise osaga – valimiste usaldus ja usaldusväärsus, riigi plaanid ning rahvusvaheline vaade. Postiloendisse on komisjoni esimees akadeemik Dan Bogdanov saatnud oma esialgse plaani konverentsi sisu kohta ja mõnede võimalike esinejate nimed. Kuna tegu on rahvusvahelise üritusega tuleb asuda läbirääkimistesse mitmete võimalike esinejatega, milleks jagatakse komisjoni liikmetele ülesanded.
   c. Samuti on vajalik rääkida kohalike esinejatega, et saaks paika konverentsi kava. Registreerimise, kutsed ja tehniliste küsimuste lahendamise võtab enda kanda akadeemia, konverents toimub salvestamisega.

Koosoleku juhataja: Dan Bogdanov

Protokollis: Ülle Sirk