CYBERNETICA

Avalik

Usaldatava täitmiskeskkonna (TEE) kasutamispõhimõtte kirjeldus muinasjututegelastega

Versioon 1.1

1 Privaatsuskaitse tehnoloogia – usaldatav täitmiskeskkond

Usaldatav täitmiskeskkond (ingl.k. *Trusted Execution Environment, TEE*) on üks privaatsuskaitse tehnoloogiatest. Ülevaadet privaatsuskaitse tehnoloogiatest saab lugeda dokumendist "Privaatsuskaitse tehnoloogiate kontseptsioon", mille koostas Cybernetica AS 2023. aastal Majandus- ja Kommunikatsiooniministeeriumi tellimusel (https://www.mkm.ee/media/8836/download).

TEE on arvuti riistvara alamosa, milles toimuv ei ole nähtav ülejäänud arvutile ja ka arvuti kasutajale. Osade TEE tehnoloogiate puhul on võimalik selle tööd ka üle arvutivõrgu kontrollida. TEE tehnoloogia võimaldab serverite sees käivitada arvutusi ja andmetöötlust, mis on isoleeritud teistest samal seadmel töötavatest arvutustest. Nii saab töödeldavaid andmeid kaitsta ka arvutit füüsiliselt kontrolliva isiku eest (näiteks sise- või välisründaja) või arvutisse paigaldatud kahjurvara eest.

Sellisest arvutist on aga vähe kasu, kui sinna lisab kaitset nõudvaid andmeid vaid selle sama arvuti haldaja. Seega vajavad TEE-d kaugatesteerimise võimalust. Atesteerimine tähendab, et väline osapool saab eemalt ühendudes tõestuse, et ta suhtleb just konkreetse TEE-ga (väldib vahendusrünnet ja õngitsusrünnet) ja selles masinas jookseb riskiosaliste poolt signeeritud kood, mida ei ole muudetud. Atesteeritud sidekanali kaudu on turvaline andmeid konkreetsesse TEE-sse laadida. Kui andmeid on vaja koguda rohkem või pikema perioodi jooksul, siis saab need TEE-s hoitava võtmega ka väljaspool TEE-d asuvasse salvestusseadmesse salvestada.

2 TEE kasutamispõhimõte

Järgnev näide on tugevalt lihtsustatud. Et detailide ligikaudsus vähem häiriks, on TEE üldpõhimõtte tutvumisel kasutatud muinasjututegelasi.

2.1 Traditsioonilise lahendus kirjeldus

Loomadel on metsas kirjade saatmiseks oma postiteenus (joonis 1 ülemine pilt). Selles postiteenuses osalevad järgmised osapooled: rebane, kilpkonnad, jänesed ja öökull.

Rebane on postiteenuse osutaja (*rebane – mingit teenust osutav server koos internetiühendusega, serveri administraatorid*). Ta kogub kirjad kokku, toob need postkontorisse ja edastab need seejärel adressaatidele. Lisaks parandab rebane ka kirjades esinevad kirjavead või tõlgib need vajadusel teise keelde.

Kilpkonnad on lõppkasutajad, kus igaühel on oma isiklik kirjavahetus.

Jänestel on perefirma, millel on ühine postkast (*jäneste postkast – asutuse infosüsteem, mis toimib asutuse sertifikaadiga*). Majasiseselt vaatavad jänesed ise, et kirjades olevad saladused oleks kaitstud ja et väljuvatel kirjadel oleks õige jänese allkiri.

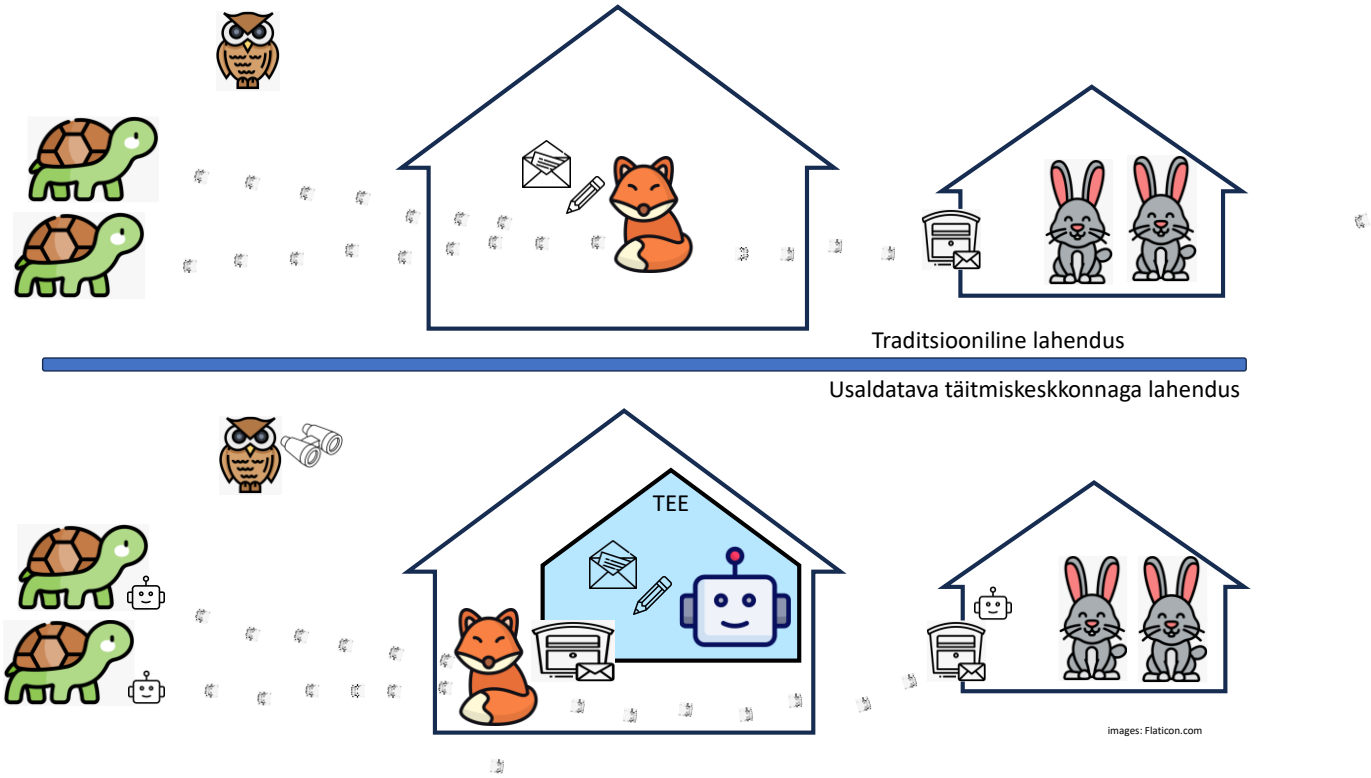
Öökull on järelevalveametnik, kes jälgivad rebase tegevust.

2.2 TEE ehk usaldatava täitmiskeskkonnaga lahenduse kirjeldus

TEE juurutamisel on rebase postkontorisse ehitatud siniste seintega TEE kast ehk usaldatav täitmiskeskkond (joonis 1 alumine pilt). TEE sisse ei pääse ükski elusolend. Seal tegutseb kindlate juhiste järgi üksnes TEE Serveri robot.

Kõikide kirjade saatmine toimub kahe sammuna:

1) kilpkonnadel ja jäneste perefirmal on väikesed TEE Kliendi robotid. Need panevad kirja saatmisel kirja kaitsvasse ümbrikusse ja kirja saamisel võimaldavad õigel kirjasaajal ümbrikku avada;
2) postkontoris avab ja töötleb kirju vaid TEE Serveri robot. Pärast kirja töötlemist paneb robot kirja uuesti kaitsvasse ümbrikusse ja rebane edastab selle jäneste postkasti.



Joonis 1. TEE juurutamise illustratsioon

2.3 Traditsioonilise lahenduse nõrkused

Loomadele traditsiooniline postiteenus küll väga meeldis, kuid sellega kaasnesid mitmed murekohad:

- kirjades oli nii isiklikke kui ka ärisaladusi, mida rebane sai põhimõtteliselt alati vaadata;
- kui võõras murdis sisse rebase postkontorisse või röövis tee peal rebaselt postikoti, sai ta kirjade sisu oma valdusesse;
- kirjasaaja ei saanud olla kindel, kes on kirja saatja, ja kas sisu on õige või vahepeal muudetud. Eriti raske oli kirja sisu usaldada siis, kui rebane oli kirja vahepeal parandanud või tõlkinud;
- öökull ei suutnud kaugelt aru saada, kas rebane teeb midagi lubamatut või mitte. Samuti nägi öökull järelevalvet tehes ka nende kirjade sisu, mida rebane parasjagu parandas või tõlkis.

Üldiselt jagunesid mured kaheks – kirjade sisu lekkimine (konfidentsiaalsus, privaatsus) ja kirjade võltsimine kurjategijate poolt (terviklus).

2.4 TEE lahenduse tugevused

Loomad leidsid olukorrale lahenduse.

- Metsaelanikud hankisid kõigile asjaosalistele robotid – rebasele kui postiteenuse osutajale suure roboti nimega TEE Server (*TEE Server – spetsiaalne riistvara ja tarkvara*), teistele väiksed robotid nimega TEE Klient (*Tee Klient – tarkvarakomponent kliendi*

arvutis/telefonis, ei nõua spetsiaalset riistvara). Kõik robotid oskasid panna kirjad sellisesse ümbrikusse, mida keegi teine peale õige roboti avada ei saanud.

- Rebase know-how vormistati TEE Serveri robotile juhendiks (*TEE juhend – TEE serveris töötav tarkvararakendus*). Juhendis olid täpselt kirjeldatud kirjade parandamise, tõlkimise ja edasisaatmise jaoks vajalikud tegevused.
- TEE Serveri roboti töö seisnes selles, et ta võttis iga talle antud kirja ümbrikust välja, vajadusel parandas või tõlkis rebase juhendi järgi ja pani valmis kirja uude ümbrikusse.
- TEE Serveri robot pandi väga erilisse purunematusse kasti nimega TEE. Kasti ehitajad kinnitasid, et kui TEE-d pidevalt hooldada, on ta praktiliselt läbimurdmatu (*TEE hooldamine – TEE vajab jooksvat turvavärskenduste installimist*).
- Enne TEE Serveri roboti tööle hakkamist pidi öökull üle vaatama kõik roboti tööjuhised ning andma vastava kinnituse ka TEE Serveri robotile, et juhend ja TEE kast on töökorras.
- TEE Serveri roboti tootja garanteeris, et robot teeb täpselt seda, mida juhend ette näeb.
- Vajadusel sai TEE Serveri roboti juhiseid muuta. Selleks tuli TEE-sse paigaldada uued juhised ja öökull pidi need heaks kiitma.
- TEE Serveri robot sai tööle hakata ning avada ja töödelda TEE Kliendi robotite poolt pakendatud ümbrikke alles siis, kui
    - TEE Serveri robotis olev juhend oli öökulli poolt heaks kiidetud. Vajadusel sai lisada ka mitu kohustuslikku heakskiitjat;
    - TEE Serveri robot tundis, et tema ümber on ikka see sama õigesti hooldatud TEE kast ja teda ei ole viidud kuskile mujale.
- TEE Kliendi robotid said kohe aru, kui neile saadetud ümbrik tuli valelt TEE Serveri robotilt.
- Öökull sai kontrollida ka kaugelt, kas TEE Serveri roboti juhised on muudetud või robot vale TEE kasti sisse pandud. TEE tootja andis talle erilise binokli, millega nägi juhiseid ka kaugelt ja mille abil sai kinnitada, et öökull näeb õige TEE kasti sees olevat TEE Serveri robotit (*binokkel – TEE tarkvara kaugatesteerimise ja signeerimise utiliit*). Samas kirjade sisu selle erilise binokliga ei näe. Sarnaselt nägid TEE Serveri roboti õigsust ka kõik TEE Kliendi robotid, kes ei pidanud selleks TEE kasti juurde kohale tulema.
- Metsloomad olid küll privaatsustundlikud, kuid siiski väga uudishimulikud metsaelu statistika osas. Nad soovisid saadetud kirjade kohta aruannet, mis oleks avalikult nähtav kõigile. Seepärast täiendati TEE Serveri roboti juhist nii, et see koostaks perioodiliselt kirjade sisu põhjal ülevaate, et mis tüüpi kirju metsaelanikud üksteisele saadavad. Näiteks kui palju armastuskirju ja kui palju arveid saadeti iga kuu. Privaatsuse kaitseks oli aruande koostamise juhis hoolikalt koostatud, et väljundist ei lekiks kellegi privaatset infot.

  Aruande avalikustamise ülesanne anti öökullile, keda metsaelanikud usaldasid. Selleks saatis TEE Serveri robot aruande kirja teel öökullile, kes avas selle TEE Kliendi robotiga ja pani seejärel kirja suure tamme tüvele kõigile vaatamiseks.

Päriselus on lahenduse reeglid erinevates situatsioonides veidi erinevad, kuid üldpõhimõte on sarnane.