# HOIA ründaja mudel

Versioon 1.0

20. august 2020

# Dokumendi ülevaade

## Kellele on dokument mõeldud?

Dokument tutvustab Eesti SARS-CoV-2 viiruse lähikontaktsete tuvastamise telefonirakenduse HOIA turvalise arendusprotsessi käigus kasutatud ründaja mudelit. Dokument eeldab lugejalt tehnilisi teadmisi tarkvaraarenduse, infoturbe ja privaatsuse kohta.

## Muudatuste ajalugu

| Versioon | Kuupäev | Märkused |
| --- | --- | --- |
| 1.0 | 20. august 2020 | Esimene avalik versioon |

## Seotud dokumendid

1. Siin dokumendis on dokumenteeritud ründaja mudel, mis kirjeldab võimalikke ründeid ja riske.
2. Dokumendihoidlas on saadaval ka turvanõudete loetelu, millele vastavalt on valitud turvameetmed.
3. Dokumendihoidlas on saadaval ka turvameetmete kirjeldus, mis kirjeldab ka meetmete valikust ja rakenduse põhimõttelistest omadustest tulenevaid jääkriske.

# Allikad

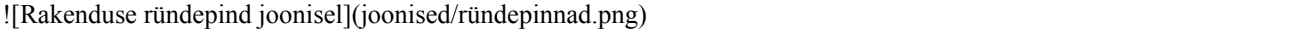
Ründaja mudeli koostamisel on võetud aluseks järgmised dokumendid, mille sisu on kohandatud Eesti oludele.

1. ENISA dokument "Cybersecurity requirements and testing for COVID-19 apps"
2. DP-3T projekti dokument "[Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems](https://github.com/DP-3T/documents/blob/master/Security analysis/Privacy and Security Attacks on Digital Proximity Tracing Systems.pdf)"

## Ründepind

[Ründepind](https://akit.cyber.ee/term/4519-rundepind) on kaitstava objekti (seadme, tarkvara, süsteemi, võrgu) täielik [nõrkuste](https://akit.cyber.ee/term/102-norkus-1) hulk või täielik [ründevektorite](https://akit.cyber.ee/term/13-rundevektor) hulk.

ENISA on kirjeldanud SARS-CoV-2 viiruse tõkestamiseks loodud rakendusele ründepinna mudeli. Allolev joonis on väljavõte ENISA dokumendist.




Hoia rakenduse ründepinnal on järgmised osad.

| Osa | Selgitus |
| --- | --- |
| i1 | Hoia rakenduse kasutaja |
| ds1 | Telefonis salvestatav ja töödeldav teave |
| p1 | Telefonis töötav rakendus |
| df1 | Nutitelefoni ja Hoia teenuse serverite vaheline ühendus |
| p2 | Hoia teenuse serverid, millega Hoia rakendus suhtleb ning mida süsteemiadministraatorid haldavad |
| ds2 | Hoia teenuse serverites salvestatavad ja töödeldavad andmed |
| df2 | Hoia teenuse serverite ja teenuse süsteemide ja nende administraatorite vaheline ühendus |
| p3 | Hoia rakenduse ja serverite arendus- ja juurutusprotsess |
| i3, i4 | Hoia rakenduse arendajad, süsteemiadministraatorid ja teenusejuhid, kes arendavad, juurutavad, seadistavad ja juhivad teenust ja selle servereid |
| ds3 | Koodihoidla, milles on Hoia rakenduse, teenusepoole ning seadistuste kood |
| df3 | Ühendus rakenduse arendajate ja rakenduste poe vahel, mille kaudu liiguvad valmisrakendus ning uuendused |

arendaja juurest rakenduste poodi |
| p4 | Rakenduste pood, mille kaudu Hoia rakendust ning selle uuendusi levitatakse |
| df4 | Ühendus nutitelefoni ja rakenduste poe vahel, mille kaudu liiguvad valmisrakendus ning uuendused rakenduste poest kasutaja nutitelefoni |

## Ohtude kataloog

### Sissejuhatus

Ohtude kataloog on toodud järgmisel kujul:

1. Rünnatav osa rakenduses - vastavalt üleval toodud tabelile.
2. Ründe tüüp - vastavalt [STRIDE](https://en.wikipedia.org/wiki/STRIDE_%28security%29) klassifikaatorile.
3. Oht - ohule antud kood ja kirjeldus.
4. Vastumeetmed/jääkriskid - turvameetmed ja jääkriskide analüüs.

Ohud on jaotatud järgmistesse gruppidesse:

1. OR - ohud, mis on põhjustatud rünnetest rakendusele ja selle kasutajale.
2. OS - ohud, mis on põhjustatud rünnetest sidekanalitele.
3. OT - ohud, mis on põhjustatud rünnetest teenuse vastu.
4. OA - ohud, mis on põhjustatud rünnetest rakenduse arendusprotsessi ja koodi vastu.
5. OP - ohud, mis on põhjustatud spetsiifilistest rünnetest kasutaja privaatsusele.

Iga ohu kohta on antud viide rakenduse turvameetmetele. Ühe kodeeritud turvameetme näol on tegemist mitmest tehnilisest ja/või organisatoorsest meetmest koosneva grupiga. Turvameetmed on täpsemalt kirjeldatud eraldi dokumendis.

### OR: Ohud, mis on põhjustatud rünnetest rakendusele ja selle kasutajale

| Rünnatav | Ründe tüüp | Oht | Vastumeetmed/jääkriskid |
| --- | --- | --- | --- |
| i1: kasutaja | Teesklus (S) | OR-1: Ründaja teeskleb suhtluses teenusega, et on mõni teine kasutaja | MR-1: Kasutaja autenditakse tugeva autentimisega<br /><br />Selgitus: näiteks esineb üks kasutaja teisena ning üritab avaldada tema eest teavet teenusele. HOIA rakenduses on selle vastu ka muud kaitsed, nt haigeks ei saa märkida kui sa haige pole. |
| i1: kasutaja | Salgamine (R) | OR-2: Kasutaja teeb rakenduses toimingu ning eitab seda pärast | MR-1: Kasutaja autenditakse tugeva autentimisega<br /><br />Selgitus: näiteks esineb kasutaja teisena ning avaldab teavet teenusele, aga pärast vaidleb teenusepakkujaga, et tema seda ei teinud. |
| ds1: andmed telefonis | Muukimine (T) | OR-3: Ründaja manipuleerib rakenduse andmetega | MR-2: Rakenduse andmete ja õigustega manipuleerimist takistatakse |
| ds1: andmed telefonis | Avalikustamine (I) | OR-4: Telefoni salvestatud andmed lekivad ründajale | MR-2: Rakenduse andmete ja õigustega manipuleerimist takistatakse <br />MR-4: Toodangurakendus peab vaid hädavajalikku logi |
| ds1: andmed telefonis | Tõkestus (D) | OR-5: Rakendus takistab ligipääsu andmetele | Mõeldud on juhtumit, kui modifitseeritud rakenduse funktsioon pahatahtlikult takistab tööd kogutud andmetega. See risk aktsepteeritakse, sest ligipääs rakenduse andmetele telefonis võib olla suurem kahju kui rakenduse mittetöötamine. |
| p1: rakendus telefonis | Teesklus (S) | OR-6: Ründaja võltsib Eesti Hoia rakenduse teistsuguse funktsionaalsusega | MO-1: Eesti riik ei luba Apple/Google rakenduste poodi koroonaviirusega seotud rakendusi ilma Sotsiaalministeeriumi kooskõlastuseta |
| p1: rakendus telefonis | Muukimine (T) | OR-7: Ründaja pöördprojekteerib rakenduse ja muudab funktsionaalsust | MT-1: Rakendustelt saadetud sisendandmeid kontrollitakse ka serveri poolel <br />MO-2: Rakenduse ja teenuse uusi versioone ei levitata või juurutata enne turvaauditit |
| p1: rakendus telefonis | Salgamine (R) | OR-8: Kasutaja salgab rakenduse tehtud päringut teenusele | MR-1: Kasutaja autenditakse tugeva autentimisega<br /><br />Selgitus: näiteks üritab rakenduse kasutaja väita, et tema ei märkinud ennast haigeks ja telefon tegi seda ise. |
| p1: rakendus telefonis | Avalikustamine (I) | OR-9: Rakenduse teostus lekib andmeid | MR-2: Rakenduse andmete ja õigustega manipuleerimist takistatakse <br />MR-3: Rakenduse andmekasutus on minimeeritud <br />MR-4: Toodangurakendus peab vaid hädavajalikku logi |
| p1: rakendus telefonis | Tõkestus (D) | OR-10: Rakenduse sidet tõkestatakse või koormatakse üle | See risk on 10. juuni 2020 seisuga aktsepteeritud risk. Tulevased versioonid võivad seda muuta. Märgime ära, et see on erisus |

võrreldes ENISA dokumendiga, mis soovitab sidekanaleid töökindlamaks muuta. |
| p1: rakendus telefonis | Õiguste vallutus (E) | OR-11: Rakendust kasutatakse telefonis kõrgemate õiguste vallutamiseks | MR-2: Rakenduse andmete ja õigustega manipuleerimist takistatakse |

### OS: Ohud, mis on põhjustatud rünnetest sidekanalitele

| Rünnatav | Ründe tüüp | Oht | Vastumeetmed/jääkriskid |
| --- | --- | --- | --- |
| df1: side rakenduse ja teenuse vahel | Muukimine (T) | OS-1: Ründaja võltsib rakenduse suhtlust teenusega | MU-1: Side toimub üle autenditud turvakanalite |
| df1: side rakenduse ja teenuse vahel | Avalikustamine (I) | OS-2: Ründaja kuulab pealt rakenduse suhtlust teenusega | MU-1: Side toimub üle autenditud turvakanalite |
| df1: side rakenduse ja teenuse vahel | Tõkestus (D) | OS-3: Ründaja koormab üle teenuse sidekanalid | MT-2: Teenusetõkestusründeid tõrjutakse nii võrgu kui liideste tasemel |
| df2: side teenuse ja teenusehalduri vahel | Muukimine (T) | OS-4: Ründaja võltsib teenusehalduri suhtlust teenusega | MU-1: Side toimub üle autenditud turvakanalite |
| df2: side teenuse ja teenusehalduri vahel | Avalikustamine (I) | OS-5: Ründaja kuulab pealt teenusehalduri suhtlust teenusega | MU-1: Side toimub üle autenditud turvakanalite |
| df2: side teenuse ja teenusehalduri vahel | Tõkestus (D) | OS-6: Ründaja koormab üle teenuse sidekanalid | MT-2: Teenusetõkestusründeid tõrjutakse nii võrgu kui liideste tasemel |
| df3: side arendaja ja rakenduste poe vahel | Muukimine (T) | OS-7: Ründaja manipuleerib rakendusega selle üleslaadimise ajal | MU-1: Side toimub üle autenditud turvakanalite <br />MA-2: Rakenduse tarnimisel rakendatakse eraldi turvameetmeid |
| df3: side arendaja ja rakenduste poe vahel | Avalikustamine (I) | OS-8: Rakendus lekib üleslaadimise ajal | MU-1: Side toimub üle autenditud turvakanalite |
| df3: side arendaja ja rakenduste poe vahel | Tõkestus (D) | OS-9: Ründaja koormab üle rakenduste poe | See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe funktsionaalsuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |
| df4: side rakenduste poe ja kasutaja telefoni vahel | Muukimine (T) | OS-10: Ründaja võltsib telefoni suhtlust rakenduste poega | MU-1: Side toimub üle autenditud turvakanalite |
| df4: side rakenduste poe ja kasutaja telefoni vahel | Avalikustamine (I) | OS-11: Rakendus lekib allalaadimise ajal | MU-1: Side toimub üle autenditud turvakanalite |
| df4: side rakenduste poe ja kasutaja telefoni vahel | Tõkestus (D) | OS-12: Ründaja koormab üle rakenduste poe ja telefonide vahelise sidekanali | See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe funktsionaalsuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |

### OT: Ohud, mis on põhjustatud rünnetest teenuse vastu

| Rünnatav | Ründe tüüp | Oht | Vastumeetmed/jääkriskid |
| --- | --- | --- | --- |
| p2: teenus serveris | Teesklus (S) | OT-1: Ründaja võltsib teenust rakenduste jaoks | MU-1: Side toimub üle autenditud turvakanalite |
| p2: teenus serveris | Muukimine (T) | OT-2: Ründaja modifitseerib teenust käituma teisiti, kui ette nähtud | MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt <br />MO-2: Rakenduse ja teenuse uusi versioone ei levitata või juurutata enne turvaauditit |
| p2: teenus serveris | Salgamine (R) | OT-3: Teenus salgab mingit tegevust või teavet | MT-4: Teenus kasutab turvalist logimist |
| p2: teenus serveris | Avalikustamine (I) | OT-4: Ründaja lekitab teenuse andmeid | MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt <br />MT-4: Teenus kasutab turvalist logimist |
| p2: teenus serveris | Tõkestus (D) | OT-5: Ründaja kasutab teenuse suunas tõkestusrünnet | MT-2: Teenusetõkestusründeid tõrjutakse nii võrgu kui liideste tasemel |
| p2: teenus serveris | Õiguste vallutus (E) | OT-6: Teenust kasutatakse juurutuskeskkonnas kõrgemate õiguste vallutamiseks | MT-5: Teenuse juurutus on isoleeritud teistest süsteemidest |
| ds2: andmed teenuses | Muukimine (T) | OT-7: Ründaja manipuleerib teenuse andmetega | MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt <br />MT-5: Teenuse juurutus on isoleeritud teistest süsteemidest |
| ds2: andmed teenuses | Avalikustamine (I) | OT-8: Ründaja lekitab teenuse andmeid | MT-3: Teenuse |

juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt |
| ds2: andmed teenuses | Tõkestus (D) | OT-9: Ründaja takistab teenuse ligipääsu andmebaasiserverile | MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt |
| i2: teenuse haldurid | Teesklus (S) | OT-10: Ründaja kehastab teenuse haldurit | MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt |
| i2: teenuse haldurid | Salgamine (R) | OT-11: Süsteemihalduri tegevust salatakse | MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt <br />MT-4: Teenus kasutab turvalist logimist |

### OA: Ohud, mis on põhjustatud rünnetest rakenduse arendusprotsessi ja koodi vastu

| Rünnatav | Ründe tüüp | Oht | Vastumeetmed/jääkriskid |
| ---------- | ---------- | ---------- | ---------- |
| p3: rakenduse arendus | Teesklus (S) | OA-1: Ründaja võltsib Eesti Hoia rakenduse arendusmeeskonna liikmelisust | MO-1: Eesti riik ei luba Apple/Google rakenduste poodi koroonaviirusega seotud rakendusi ilma Sotsiaalministeeriumi kooskõlastuseta <br />MO-3: Rakenduse ja teenuse uusi versioone tarnib TEHIK |
| p3: rakenduse arendus | Muukimine (T) | OA-2: Ründaja manipuleerib rakenduse arendusmeeskonnaga | MO-2: Rakenduse ja teenuse uusi versioone ei levitata või juurutata enne turvaauditit <br />MO-5: Projektil on selge juhtimisstruktuur |
| p3: rakenduse arendus | Salgamine (R) | OA-3: Ründaja teeb rakenduse arenduses või juurutamises tegevuse ning salgab seda | MA-1: Arenduskeskkonnale ligipääs on autenditud ning pääsuõigustega |
| p3: rakenduse arendus | Avalikustamine (I) | OA-4: Ründaja lekitab teavet arenduskeskkonnast | MO-4: Teabe avalikustamist kooskõlastab Sotsiaalministeerium |
| p3: rakenduse arendus | Tõkestus (D) | OA-5: Ründaja koormab üle arendus- või juurutusmeeskondade ressursid | MO-5: Projektil on selge juhtimisstruktuur <br />Jääkriski analüüs: Märkimist vääriv jääkrisk on konsortsiumi ettevõtete töötamine vabatahtlikkuse alusel. TEHIKu ressursse saab Sotsiaalministeerium juhtida, aga ettevõtete juhtimine käib õhinapõhisuse ja mittevaralise motiveerimise alusel. |
| p3: rakenduse arendus | Õiguste vallutus (E) | OA-6: Ründaja kasutab ära arendus- või juurutusmeeskonda, et saada ligipääsu piiratud ressurssidele | MA-1: Arenduskeskkonnale ligipääs on autenditud ning pääsuõigustega <br />MT-3: Teenuse juurutus on kaitstud tervishoiuinfosüsteemidele kehtivate nõuete kohaselt <br />MT-5: Teenuse juurutus on isoleeritud teistest süsteemidest |
| ds3: rakenduse kood | Muukimine (T) | OA-7: Ründaja manipuleerib rakenduse koodi või seadistustega | MA-1: Arenduskeskkonnale ligipääs on autenditud ning pääsuõigustega <br />Märkus: tulevikuversioonides tuleks kaaluda ka lähtekoodi signeerimist |
| ds3: rakenduse kood | Avalikustamine (I) | OA-8: Ründaja avalikustab rakenduse koodi | Silmas peetakse avalikustamiseks mitte ette nähtud (nt auditeerimata) koodi avalikustamist. <br />MO-4: Teabe avalikustamist kooskõlastab Sotsiaalministeerium |
| ds3: rakenduse kood | Tõkestus (D) | OA-9: Ründaja tõkestab ligipääsu rakenduse koodile | See risk on 11. juuni 2020 seisuga aktsepteeritud risk. Tulevased versioonid võivad seda muuta. Rakenduse koodile ligipääs ei ole ajakriitiline, kui vaid mainekujunduse mõttes. |
| i3: arendajad | Teesklus (S) | OA-10: Ründaja kehastab rakenduse arendajat | MA-1: Arenduskeskkonnale ligipääs on autenditud ning pääsuõigustega |
| i3: arendajad | Salgamine (R) | OA-11: Rakenduse arendaja tegevust salatakse | MA-1: Arenduskeskkonnale ligipääs on autenditud ning pääsuõigustega |
| p4: rakenduste pood | Teesklus (S) | OA-12: Ründaja kehastab rakenduste poodi | MU-2: Teavitustegevus nutitelefonide turvahügieenist <br />See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe usaldatavuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |
| p4: rakenduste pood | Muukimine (T) | OA-13: Ründaja manipuleerib rakenduste poe andmetega | See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe usaldatavuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |
| p4: rakenduste pood | Salgamine (R) | OA-14: Rakenduste pood salgab tehtud toimingut | See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe usaldatavuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |
| p4: rakenduste pood | Avalikustamine (I) | OA-15: Rakenduste pood lekib andmeid | See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe konfidentsiaalsuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |
| p4: rakenduste pood | Tõkestus (D) | OA-16: Ründaja takistab ligipääsu rakenduste poele | See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe käideldavuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |
| p4: rakenduste pood | Õiguste vallutus (E) | OA-17: Ründaja vallutab rakenduste poe taristul kõrgendatud ligipääsu |

See risk on 13. juuni 2020 seisuga aktsepteeritud risk. Me eeldame, et rakenduste poe usaldatavuse kaotamine on valitud platvormide haldajatele (Apple, Google) nii suur risk, et neil on vastumeetmed juurutatud. |

### OP: Ohud, mis on põhjustatud spetsiifilistest rünnetest kasutaja privaatsusele

| Rünnatav | Ründe tüüp | Oht | Vastumeetmed/jääkriskid |
| ---------- | ---------- | ---------- | ---------- |
| i1: kasutaja | Muukimine (T) | OP-1: Ründaja loob uusi kontakte, mida tegelikult pole olnud (DP-3T riskianalüüsi riskid GR1 ja GR2) | MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Seda riski ei saa lõpuni kahandada, sest see on Bluetooth-signaale kasutava kontaktide tuvastamise süsteemi omadus. <br />Jääkriski analüüs: ründaja, kellel on võimas Bluetooth-antenn, saab tugevdada mõne isiku (nt ka haigestunud isiku) rakenduse levitatavaid signaale, tekitades võltsteavitusi teistele inimestele, kes pole tegelikult haigega kontaktis olnud. Selline rünne kahandaks usaldust rakenduse vastu. Selle läbiviimine nõuab koostööd haigestunud isikuga, kes pole veel ennast rakenduses haigeks märkinud ning seda võib käsitleda kui teise inimese pahatahtlikku nakatamist, kui sellise haigestunuga käia nt rahvarohkes kohas "signaale levitamas". Seega seega on sellise teguviisi kahjud võimaliku ründaja jaoks märkimisväärsed. Märgime ka ära, et see rünne ei skaleeru hästi, sest kulutab ründajal päris palju aega. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (riskid GR1 ja GR2). |
| i1: kasutaja | Muukimine (T) | OP-2: Ründaja manipuleerib kasutaja telefonis andmetega, et nt märkida ta riskigruppi kuuluvaks, et ta saaks teavituse (DP-3T riskianalüüsi risk SR2) | MU-2: Teavitustegevus nutitelefonide turvahügieenist <br />MR-2: Rakenduse andmete ja õigustega manipuleerimist takistatakse <br />Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk SR2). |
| i1: kasutaja | Avalikustamine (I) | OP-3: Mõnele isikule saab teatavaks, kellega mõni rakenduse kasutaja pikemaajalises kontaktis on olnud ehk kontaktide graaf (DP-3T riskianalüüsi risk SR1) | MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Jääkriski analüüs: kui ründaja (riik või eraisik) seab üles laiaulatusliku Bluetooth antennide süsteemi ning suudab siduda kogutud signaale nende isikutega, on tal võimalik selline info tuvastada. Märgime ära, et samasugune rünne on võimalik läbi viia ka ilma rakenduseta ning rakendus ei tõsta vastava ohu tõenäosust. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk SR1). |
| i1: kasutaja | Avalikustamine (I) | OP-4: Mõnele isikule saab teatavaks, kelle lähedal mõni rakenduse kasutaja on olnud (läheduse graaf) | MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Jääkriski analüüs: kui ründaja (riik või eraisik) seab üles laiaulatusliku Bluetooth antennide süsteemi ning suudab siduda kogutud signaale nende isikutega, on tal võimalik selline info tuvastada. Märgime ära, et samasugune rünne on võimalik läbi viia ka ilma rakenduseta ning rakendus ei tõsta vastava ohu tõenäosust. |
| i1: kasutaja | Avalikustamine (I) | OP-5: Mõnel isikul on võimalik rakendust kasutavate nakatunud inimeste asukohti tuvastada (DP-3T riskianalüüsi risk GR3) | MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Jääkriski analüüs: selliseks ründeks kombineerib ründaja OP-2, OP-3 ja OP-8 tehnikaid, sõites ringi ja tuvastades asukohti, kus on nakatunud kasutajad. Rünne on sama (eba)efektiivne kui nimetatud tehnikad. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk GR3). |
| i1: kasutaja | Avalikustamine (I) | OP-6: Mõnel isikul on võimalik tervete rakendust kasutavate inimeste asukohta jälgida (osaliselt DP-3T riskianalüüsi risk SR3) | MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Jääkriski analüüs: rakendus ei kasuta inimeste asukohaandmeid (nt GPS, Wifi) ja seega ei tee kellegi jälitamist lihtsamaks ei riigile ega eraisikutele. Kui ründaja (riik või eraisik) seab üles laiaulatusliku Bluetooth antennide süsteemi, siis suudab ta ühe ajutise võtme kehtivusaja jooksul (10-20 minutit) raadiosignaali järgi liikumist jälgida. Seejärel võti muutub ning kahte võtit ühendada (et jätkata sama inimese jälitamist) ründaja ei suuda. Rünne on tugevam, kui eelnevalt õnnestub kätte saada päevavõti, millest ajutisi võtmeid arvutatakse. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk SR3). |
| i1: kasutaja | Avalikustamine (I) | OP-7: Mõnel isikul on võimalik rakenduse haigestunud kasutajaid tuvastada | MU-2: Teavitustegevus nutitelefonide turvahügieenist <br />MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Jääkriski analüüs: kasutaja märgib ennast teenuses haigeks ise, saades vastava kinnituse tervishoiusüsteemist. Seega "rakenduse kaudu" lekib haiguse teave vaid siis, kui kasutajat jälgiv isik märkab, et kasutaja on jäänud haigeks või raporteerib ennast haigeks rakenduses, näiteks üle õla tema tegevust jälgides. Selline tegevus ei võimalda rünnata paljusid inimesi korraga, kuid võib tekitada kahjusid üksikutele kasutajatele. |
| i1: kasutaja | Avalikustamine (I) | OP-8: Võimaliku nakatumise kohta teavituse saanud rakenduse kasutaja võib olla võimeline tuvastama, milliselt oma kontaktilt ta nakkuse sai (DP-3T riskianalüüsi risk IR1) | Rakendus ei näita selle isiku infot, kellega kontakti saadi, sest rakendus ei tea seda. Samas, seda riski ei saa lõpuni kahandada, sest see on teavitusi tegeva kontaktide tuvastamise süsteemi põhiomadus. <br />Jääkriski analüüs: Seda riski ei ole võimalik lõpuni kahandada, sest alati jääb võimalus, et kui inimesel on olnud vaid üks kontakt, siis see pidi olema nakatunud isikuga. Lahenduse põhimõtteks jääb, et püütakse tuvastada kontakte mitmete võõraste inimeste hulgas liikumisel. Selline oht ei ole seotud rakendusega, vaid on kontaktijälgimise fundamentaalne omadus. Iga selline süsteem saab ehitada sisse teatud hulga piiranguid, et teha võimaliku nakataja tuvastamist keerukamaks ja siin on Eesti rakenduse eelis see, et kuskil pole keskset andmebaasi, mis võimaldaks sellist rünnet teha massiliselt. Risk on süvendatud juhul, kui kasutatakse murtud operatsioonisüsteemi. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk IR1). |

| i1: kasutaja | Avalikustamine (I) | OP-9: Ründaja võib jälgida nutitelefonide kasutajaid nende teiste võrguidentifikaatorite abil (DP-3T riskianalüüsi risk GR5) | MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Seda riski ei saa lõpuni kahandada, sest see on Bluetooth-signaale kasutava kontaktide tuvastamise süsteemi omadus. <br />Jääkriski analüüs: Tundlike raadioantennidega varustatud süsteemne isik võib sõita läbi linna ja kaardistada mobiiltelefone, mis Bluetooth või muid (nt WiFi) signaale levitavad. Selline tegevus kannab WiFi kontekstis nime wardriving ja võimaldab süsteemsel isikul kaardistada inimeste asukohti. Kui seda teha väga süsteemselt, võimalikke haigeid inimesi jälitades, võib hea õnnega tuvastada kohti, kus haige inimene on käinud. Rünne on ressursikulukas ning efekt saavutatav ka lihtsalt sotsiaalmeedias valeväitega, a la "Ülemiste keskuses käib palju koroonahaigeid". Seega rakendus ei tee seda rünnet lihtsamaks kui see muidu on. Uuemad seadmed võtavad iga 10-20 minuti tagant kasutusele ka uue Bluetooth Low Energy MAC aadressi. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk GR5). |
| i1: kasutaja | Avalikustamine (I) | OP-10: Ründaja võib jälgida nutitelefoni suhtlust teenusega ning selle järgi kontekstist tuvastada kasutaja tegevusi selles (DP-3T riskianalüüsi risk NR2) | MR-1: Kasutaja autenditakse tugeva autentimisega <br />MU-3: Kasutatakse hajusat kontaktijälgimise protokollistikku <br />Jääkriski analüüs: Mobiilside ja WiFi-alade operaatorid näevad telefonide liiklust ning võivad analüüsida selle mustreid. Nt kas inimene käib teatud veebilehtedel või suhtleb teatud teenusepakkujatega. Eesti rakenduse puhul on suhtlus teenusepakkujatega kavandatud nii, et suhtlemise kontekst ise ei lekita vastavat infot. Diagnoosi kinnitamiseks logib telefoni kasutaja sisse patsiendiportaali, mida ta võib teha ka muudel otstarvetel. DP-3T protokoll on kavandatud nii, et terve ja haigestunud inimese side ei erine. Märgime ära, et sideoperaatoritel on lihtsamaid võimalusi tuvastada isiku terviseseisundit (nt kui avalikus WiFi võrgus otsitakse internetist "koroonaviiruse sümptom maitsetaju"). See rünne ei vaja rakendust. Soovitame kõigil alati jälgida, kas veebiteenuseid kasutatakse üle turvaliste ühenduste (https:// aadressid, kinnised tabalukud veebibrauseri aadressreal). Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk NR2). |
| i1: kasutaja | Avalikustamine (I) | OP-11: Ründaja saab teada, et kasutaja kasutab rakendust (DP-3T riskianalüüsi risk GR6) | See risk on aktsepteeritud. Kommunikatsioon rõhutab, et rakenduse kasutajad aitavad ühiskonnas haigust tõrjuda ning sellises õhkkonnas antud tegevuses osalemist ei peeta diskrimineerivaks. Olukord oleks erinev, kui tegemist oleks nt immuunsuspassi tüüpi rakendusega. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk GR6). |
| i1: kasutaja | Avalikustamine (I) | OP-12: Teenusepakkuja saab teada, milline kasutaja on haigestunud (DP-3T riskianalüüsi risk NR1) | See risk on aktsepteeritud. Eestis on rakendus teenuse omanik Terviseamet, kes kasutab selle käitamiseks TEHIKu teenuseid. Terviseameti infosüsteemides on diagnoositud haiged nagunii teada. Olukord oleks erinev, kui Eestis puuduks keskne e-tervise infosüsteem TIS. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk NR1). |
| i1: kasutaja | Avalikustamine (I) | OP-13: Lahti muugitud telefon võimaldab täiendavaid ründeid konfidentsiaalsuse vastu | MU-2: Teavitustegevus nutitelefonide turvahügieenist <br />MR-2: Rakenduse andmete ja õigustega manipuleerimist takistatakse <br />Jääkriski analüüs: kui kasutaja telefon on lahti muugitud (_jailbroken_, _rooted_), siis võib ründaja pääseda ligi võtmetele, mis vähendavad meetme MU-3 efektiivsust. Kuigi Apple/Google APIde kasutus kaitseb neid võtmeid, siis lahti muugitud telefonides need kaitsed nii efektiivsed ei ole ning see muudab tõsisemaks riski OP-1, OP-2, OP-5 |
| i1: kasutaja | Tõkestus (D) | OP-14: Kasutaja takistab kontaktide loomiseks vajalikke signaale (DP-3T riskianalüüsi risk IR2) | Seda riski ei saa lõpuni kahandada, sest see on Bluetooth-signaale kasutava kontaktide tuvastamise süsteemi omadus. Lisaks peab telefoni kasutaja ise saama seda funktsiooni välja lülitada, et säiliks rakenduse vabatahtlikkus. <br />Jääkriski analüüs: kui kasutaja lülitab lähikontaktsete tuvastamiseks vajaliku raadioside ise välja, on see tema vaba valik, mis peab säilima. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk IR2). |
| i1: kasutaja | Tõkestus (D) | OP-15: Ründaja takistab kontaktide loomiseks vajalikke signaale (DP-3T riskianalüüsi risk GR4) | Seda riski ei saa lõpuni kahandada, sest see on Bluetooth-signaale kasutavakontaktide tuvastamise süsteemi omadus. <br />Jääkriski analüüs: Ründaja kasutab raadiosegajat, et takistada nt haigestunud isiku rakendust signaale levitamast ja nii tekitada nakatumisi, mida rakendus "ei leiaks". Ka selline tegevus on tõlgendatav inimeste pahatahtliku nakatamisena, seega on sellise teguviisi kahjud võimaliku ründaja jaoks märkimisväärsed. Selline rünne on samas palju mõistlikum teha nii, et nakatunud inimene, kellega on vaja koostööd teha, et temaga koos Bluetooth-segajat kaasa vedada, jätab lihtsalt telefoni koju ja käib hingab teiste suunas. Seega see rünne on rakendusega võimalik, aga ilma selleta lihtsamgi. Pikemat käsitlust saab lugeda DP-3T turvaanalüüsist (risk GR4). |