

TALLINNA TEHNIKAÜLIKOOL  
Infotehnoloogia teaduskond  
Tarkvarateaduse instituut

Heiko Parmas 142272

**VIRTUAALSE IDENTITEEDIGA SEOTUD  
RÜNDED JA KAITSE TTÜ VIRTUAALSETE  
ÕPIKESKKONDADE NÄITEL**

Bakalaureusetöö

Juhendaja: Sten Mäses, MSc

Tallinn 2017

## **Autorideklaratsioon**

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Heiko Parmas

22.05.2017

## **Annotatsioon**

Töö eesmärk on analüüsida ja kaardistada virtuaalidentiteediga seotud rünnakuid erinevates e-õppekeskkondades TTÜ infosüsteemide näitel.

Lisaks toob antud töö välja virtuaalidentiteedi kasutuskohad TTÜ süsteemides, potentsiaalsed rünned virtuaalidentiteedile ning tutvustab erinevaid identifitseerimismeetodeid. Rünnete vastu kaitsena pakutakse töös välja lahendus identifitseerimissüsteemi näitel, millega saaks potentsiaalselt tuvastada ründeid ning tuvastatud rünnete puhul vähendada ründega seotud riske.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 23 leheküljel, 10 peatükki, 7 joonist, 1 tabelit.

## **Abstract**

### **Virtual identity related attacks and defence on the example of TUT online learning environments**

Goal of the thesis is to analyse and map attacks related to virtual identity in different online learning environments on the example of TUT information systems.

In addition this thesis brings out the uses of virtual identity in different TUT systems, potential attacks on virtual identity and introduces different identification methods. As a defence against the potential attacks, this thesis offers a solution on the example of an identification system that could potentially detect attacks and help alleviate risks related to successful attacks.

The thesis is in Estonian and contains 23 pages of text, 10 chapters, 7 figures, 1 tables.

## Lühendite ja mõistete sõnastik

|            |   |
|------------|---|
| IP aadress | <i>Internet Protocol address</i><br>Arvuti aadress internetis |
| Uni-ID     | TTÜ digitaalne identiteet                                     |
| TTÜ        | Tallinna Tehnikaülikool                                       |
| HITSA      | Hariduse Infotehnoloogia Sihtasutus                           |
| ÕIS        | Õppeinfosüsteem   |

## Sisukord

|   |    |
|---|----|
| 1 Sissejuhatus .....  | 10 |
| 2 Identiteet veebikeskkonas .....   | 11 |
| 2.1 Reaalse isikuga seotud identiteedid veebikeskkonas.....                           | 11 |
| 3 Identiteedivargus .....   | 12 |
| 3.1 Identiteedipettus.....  | 12 |
| 4 TTÜ-s kasutusel olevad veebikeskkonnad .....  | 13 |
| 4.1 ÕIS – Õppeinfosüsteem.....  | 13 |
| 4.2 Mail.ttu.ee .....   | 13 |
| 4.3 TTÜ IT ained .....  | 13 |
| 4.4 Pass.ttu.ee .....   | 14 |
| 4.5 HITSA Moodle .....  | 14 |
| 4.6 Maurus .....  | 14 |
| 5 Virtuaalidentiteet TTÜ kontekstis .....   | 15 |
| 6 TTÜ kontekstis virtuaalidentiteediga seotud ründed.....                             | 16 |
| 6.1 Kellegi teise eest testi tegemine.....  | 16 |
| 6.2 Teiste kulul grupitööde sooritamine .....   | 16 |
| 6.3 Veebikeskkonna identiteedivargus .....  | 17 |
| 6.3.1 Pahatahtlik veebitesti sooritamine .....  | 17 |
| 6.4 Omakasu eesmärgil virtuaalidentiteedi ärakasutamine .....                         | 17 |
| 7 Viisid virtuaalidentiteedivarguse tõkestamiseks .....                               | 18 |
| 7.1 Alternatiivne parooli valimise lahendus .....                                     | 19 |
| 8 Jooksvalt identiteedi kontrollimine .....   | 21 |
| 8.1 Näotuvastus .....   | 21 |
| 8.2 Silmad.....   | 21 |
| 8.3 Trükkimine .....  | 22 |
| 8.3.1 Nutiseadmes trükkimine .....  | 22 |
| 9 Virtuaalidentiteedi ründe analüüs ning kaitse võimalused veebitestide keskkonnas .. | 23 |
| 9.1 Tavalise kasutaja kasutusjuht .....   | 23 |
| 9.2 Ründe analüüs.....  | 24 |

|   |    |
|---|----|
| 9.2.1 Varasta ID-kaart .....                                | 24 |
| 9.2.2 Arva parool ära .....                                 | 25 |
| 9.2.3 Pane keegi ütlema oma parool.....                     | 25 |
| 9.2.4 Häki andmebaasi, kus on kasutajate info .....         | 26 |
| 9.2.5 Piilu kasutajanimi ja parool üle õla .....            | 26 |
| 9.2.6 Sisse logitud arvuti .....                            | 27 |
| 9.3 Kaitse virtuaalidentiteedi varastamise ründele .....    | 27 |
| 9.4 Virtuaalidentiteedi varastamise ründe tuvastamine ..... | 28 |
| 9.4.1 Klahvivajutuste jälgimine.....                        | 29 |
| 9.4.2 Näotuvastus .....                                     | 29 |
| 9.4.3 Korduv autentimine .....                              | 30 |
| 9.4.4 Silmaiirise skaneerimine .....                        | 30 |
| 10 Kokkuvõte .....  | 32 |
| Kasutatud kirjandus .....                                   | 33 |

## Jooniste loetelu

|  |    |
|--|----|
| Joonis 1. Parooli valimise atribuudid .....  | 18 |
| Joonis 2. LastPassi parooli genereerimise kasutajaliides .....                       | 20 |
| Joonis 3. Kasutaja kulg testikeskkonnas .....  | 23 |
| Joonis 4. Hea- ja pahatahtliku võõra identiteedi kasutaja kulg testikeskkonnas ..... | 23 |
| Joonis 5. Virtuaalidentiteedi varastamise ründepuu .....                             | 24 |
| Joonis 6. Kasutaja kulg turvalisemas testikeskkonnas .....                           | 28 |
| Joonis 7. Kasutaja kulg identifitseerimissüsteemiga keskkonnas .....                 | 28 |



## **Tabelite loetelu**

|  |    |
|--|----|
| Tabel 1. Atribuutide valikud ja näited ..... | 19 |
|--|----|

## 1 Sissejuhatus

Identiteet on miski, mis ideeliselt peaks aitama eristada inimesi. Seda joont üritatakse ületada sooritades identiteedivargust, olgu see kas reaalses maailmas või veebis. Identiteedivarguse puhul on tegu üheselt defineerimatu kontseptiga, millele täpseid piire ei ole võimalik määrata.

TTÜ-s on kasutusel virtuaalidentiteedid, mis ideeliselt hõlbustavad tööd nii õppe kui ka administratiivsel tasandil, luues võimaluse edastada isikustatud infot ilma otsese isikliku kokkupuuteta. TTÜ kontekstis on identiteedivargus kellegi virtuaalidentiteedi kasutamine pahatahtlikul eesmärgil. Selline tegevus võib väljenduda õppejõu identiteedi kasutamises paremate õpitulemuste saamiseks, kui ka veebitestide kellegi teise eest pahatahtlikult sooritamises.

TTÜ kontekstis on virtuaalidentiteet suuresti kasutusel veebitestide sooritamisel. Veebitestide tegemisel virtuaalidentiteedi kaitsmiseks tuleks kasutada erinevaid identifitseerimismeetodikaid, et hoida ära identiteedivargust. Töö eesmärgiks on pakkuda teoreetilist lahendust virtuaalidentiteedi rünnakute tuvastamiseks ja tõkendamiseks.

## 2 Identiteet veebikeskkonas

Igal veebikülastajal on tahes tahtmata oma identiteet. Identiteet võib olla seotud kas veebiaadressiga (IP), reaalse aadressiga (tänav, maja number jne), reaalse isikuga (nimi, isikukood jne) või virtuaalse isikuga (enda poolt valitud kasutajanimi). Iga identiteet on seotud vähemalt ühega nendest, näiteks IP aadressiga, sest muidu ei teaks server kellele veebilehe infot saata. On ka olemas identiteedi varjamiseks välja mõeldud süsteem TOR, mille eesmärk on teha veebikülastaja anonüümseks. TOR-i kasutades ei ole praegusel hetkel võimalik täpselt positsioneerida veebikülastaja asukohta ega analüüsida tema „jalajälgi“ veebis [1].

Kõige levinum identiteedi vorm veebilehtede külastamisel on virtuaalne isik. See kujutab endast kasutaja loomist. Kasutaja loomisel palutakse sisestada identifitseerimiseks vajalik info näiteks kasutajanimi ja parool. Lisaks on tihti ka võimalus sisestada enda kohta meta-infot, mille järgi saad rohkem kujundada oma identiteeti sellel veebilehel näiteks vanus, sugu või perekonnaseis. Väga levinud on ka e-maili küsimine kasutajale info saatmise eesmärgil. Kui info on sisestatud vastava veebilehe registreerimise vormile sobivalt, siis luuakse andmebaasis kirje selle kasutaja kohta ning seda on võimalik edaspidi kasutada identiteedina sellel veebilehel.

### 2.1 Reaalse isikuga seotud identiteedid veebikeskkonas

Erinevalt enamusest veebilehtedest, on olemas veebilehti, mis nõuavad kasutaja sidumist reaalse isikuga. Paljud selliste nõuetega veebilehed kuuluvad erinevatele pankadele või riigile. Nendel lehtedel on identiteet otseselt seotud reaalse isikuga. Selle seose tekitamiseks luuakse kasutaja isikuga füüsilisel kohtumisel, näiteks panga veebilehele sisenemiseks vajaliku kasutaja loomiseks on vaja külastada vastava panga esindust. Eestis on kasutusel veebis identifitseerimiseks ka ID-kaart, mis kujutab veebis endast seost reaalse isikuga. Eesti seadusruumis on ID-kaardiga antud allkirjal juriidiline tähendus. *Digitaalallkirja olemust ning selle kasutamist reguleerib Eestis "Digitaalallkirja seadus" ehk lühidalt DAS, mis võeti vastu 7. märtsil 2000. aastal. Digiallkiri on seaduse silmis võrdne omakäelise allkirjaga.* [2]

### 3 Identiteedivargus

Identiteedivargusel puudub täpne ühene definitsioon. Eesti seadusruumis on Karistusseadustikus defineeritud identiteedivargus järgnevalt §157<sup>2</sup>: „Teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nendele juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele, või varjata kuritegu“ [3].

Veebis, nagu ka reaalses maailmas, võib anda kellegi teisenä esinemine mitmeid eeliseid. Veebis väljenduvad sellised eelised enamjaolt ligipääsuga rohkemale infole kasutajate kohta, või võimalus veebilehte muuta vastavalt oma soovidele. Sellise juhtumi tuvastamine on väga keeruline, kui ei ole võimalik reaalse asitõenditega tõendada juhtunut, näiteks videosalvestus või pildid.

#### 3.1 Identiteedipettus

Tahtlikult kellelgi teise lubamine oma kasutaja kasutamiseks on enamjaolt veebilehtede ja infosüsteemide kasutustingimustes kirjeldatud ning ka keelatud, sest eeldatakse, et iga kasutaja on seotud ainult ühe persooniga. Veebitestide kontekstis saab kellegi teise lubamist oma kasutajaga siseneda ära kasutada paremate tulemuste saamiseks. Selliseks teoks võib motiveerida paremate õpitulemuste soovimine võimalikult lihtsalt. Tegu on ühtlasi ka riskantse viisiga oma õpitulemuste parandamiseks.

## **4 TTÜ-s kasutusel olevad veebikeskkonnad**

TTÜ's on kasutusel mitmeid veebikeskkondi, mida erinevad õppejõud ja tudengid kasutavad kooliga seoses.

### **4.1 ÕIS – Õppeinfosüsteem**

TTÜ kasutab õppetööga seotud info administreerimiseks keskkonda ÕIS ehk õppeinfosüsteem, mis asub veebilehel ois.ttu.ee. Selles keskkonnas on tudengil võimalik näiteks esitada erinevaid avaldusi, tutvuda erialade, õppekavade ja ainetega, näha oma hindeid, näha oma tunniplaani, registreeruda eksamitele ja palju muud. 07.06.2016 tuli välja ÕISi teine versioon, mis asub uuel veebilehel ois2.ttu.ee, mis tegi keskkonna autori arvates kasutajasõbralikumaks. Mõlemal veebilehel on identifitseerimiseks kasutusel kasutajanime ja parooli kombinatsiooni kui ka ID-kaardi ja Mobiil-ID lahendused. [4] [5]

### **4.2 Mail.ttu.ee**

Mail.ttu.ee näitel on tegu Microsofti poolt pakutava Office 365 teenuse osaga mis pakub erinevaid pilveteenuseid. Keskkonda sisenemiseks on vaja sisestada oma UNI-ID e-mail ja parool. [6]

### **4.3 TTÜ IT ained**

TTÜ IT ained keskkonnas, veebilehel ained.ttu.ee, on võimalik õppejõul jagada õppetööga seotud materjale, luua erinevaid teste, hallata kursuse üleüldist käiku ja palju muud. Tudengil on võimalik loodud materjale vaadata või alla laadida, sooritada teste ja palju muud. TTÜ IT ained keskkonda sisenemine käib UNI-ID'd kasutades. [7]

#### **4.4 Pass.ttu.ee**

Pass.ttu.ee on TTÜ UNI-ID konto iseteeninduskeskkond, kus on võimalik hallata oma UNI-ID kontot. Keskkonda on võimalik siseneda kasutajanime ja parooli või ID-kaardi ja mobiil-ID lahendustega. Tähtis on märkida, et UNI-ID konto parooli saab ainult siis muuta, kui oled sisenenud keskkonda kasutades ID-kaardi või mobiil-ID lahendust. Seda eeldatavasti just identiteedivarguse tõkestamiseks. [8]

#### **4.5 HITSA Moodle**

HITSA Moodle on Eesti Vabariigi poolt asutatud sihtasutus, mille eesmärkidesse kuuluvad „kaasaegsete tehnoloogiate, sealhulgas info- ja kommunikatsioonitehnoloogia (edaspidi IKT), rakendamise kaudu aidata kaasa hariduse ning teadus- ja arendustegevuse kvaliteedi ning tulemuslikkuse tõusule“, „toetada IKT alase hariduse edendamist kõikidel haridustasemetel“, „tagada riiki katvate e-teadusinfrastruktuuride ja –teenuste toimimine ja areng kooskõlas tehnoloogia üldise arenguga.“ [9]. Mitmed TTÜ õppejõud kasutavad seda keskkonda oma kursusega seotud materialide jagamiseks ning kursuse üleüldiseks administreerimiseks. Keskkond asub veebilehel moodle.hitsa.ee. Keskkonda sisenemiseks saab kasutada kasutajanime ja parooli, ID-kaarti või mobiil-ID'd ja Eesti haridus- ja teadusasutustevahelise autentimise ja autoriseerimise taristu teenust ehk TAAT'i [10].

#### **4.6 Maurus**

TTÜ Tarkvaraarenduse Instituudi poolt hallatav veebikeskkond Maurus, mis asub veebilehel maurus.ttu.ee, kujutab endast HITSA Moodle ja TTÜ IT ained keskkondadega analoogilisi võimalusi pakkuvat keskkonda. Sisenemine käib kasutajanime ja parooliga. [11]

## 5 Virtuaalidentiteet TTÜ kontekstis

TTÜ siseselt kasutatakse üldiseks tudengite identifitseerimiseks, peale nende nime ja isikukoodi, neile kooli astudes antud üliõpilaskoodi. Antud kood on unikaalne ning seotud just selle reaalse isikuga, kellele see kooli pääsedes omistati. Seda koodi kasutatakse õppejõudude poolt vahel näiteks kontrolltöö tegija identifitseerimiseks. Veel on kood kasutusel TTÜ veebikeskkonnas ÕISis [4] [5], kus kasutajanime osaks on eelnimetatud üliõpilaskood.

Veel on TTÜ's kasutusel UNI-ID, mille saab üliõpilane ise endale veebis luua [8]. Selle abil on võimalik näiteks sisse logida TTÜ veebitestide keskkonda [12], kus on õppejõududel võimalik üles seada oma aine ning selle raames teha tudengitele teste. Leht pakub ka võimalusi üleüldiseks infoedastuseks aine raames. Samuti saab UNI-ID'd kasutada sellega seotud meiliteenusesse [6] sisselogimiseks, et näha vastavale e-mailile saadetud kirju.

## **6 TTÜ kontekstis virtuaalidentiteediga seotud ründed**

Ründeid virtuaalsele identiteedile TTÜ kontekstis on mitmeid. Järgnevalt toon välja nendest mõned.

### **6.1 Kellegi teise eest testi tegemine.**

TTÜ veebitestide keskkonnas ei toimu pidevat identifitseerimist. See tähendab seda, et sisse on vaja logida ühe korra ning pimesi usaldatakse sisselogitavat kasutajat. Peale sisse logimist ei kontrollita pidevalt, kas sisse loginud kasutaja on tõesti see, kelleks ta ennast esitleb. Selle nii-öelda turvavea tõttu on võimalik üliõpilastel lasta kellelgi teisel veebikeskkonnas enda eest teste teha. Sellele rünnakule lihtsat kaitset ei ole, sest hilisem testi uuesti läbi viimine kontrollitud keskkonnas ei pruugi anda kaugeltki samu tulemusi, sest paljud üliõpilased õpivad iga testi jaoks erinevalt ning pikaajalist kinnistamist ei pruugi tegelikult toimuda, mispärast ei pruugi õpilane hiljem sama testi kohta omada samu teadmisi, mis tollel ajahetkel. Kui õppejõu soov ongi välja „juurida“ õpilased, kes ei ole omandanud vastavaid teadmisi süvitsi, siis ei ole tegelikult algsel veebitestil mingisugust mõtet. Selle lihtsa põhjuse pärast on selline „vasturünnak“ autori arvates ebapraktiline.

### **6.2 Teiste kulul grupitööde sooritamine**

Mõned ülesanded TTÜ veebitestide keskkonnas on mõeldud grupis tegemiseks. Tihti soovitakse sellistele ülesannetele vastuseks üleslaaditavat faili, mis sisaldab töö tegijate nimesid. Võib tekkida võimalus, kus osa grupist on olude sunnil teinud ära terve ülesande ning jätnud töös mitte osalenud õpilaste nimed kirjutamata. Antud süsteemis ei ole hetkel võimalust vältida potentsiaalset olukorda, kus nii-öelda laisk õpilane laeb usinate õpilaste poolt lisatud töö endale arvutisse, lisab enda nime tööle ning seejärel laeb selle uuesti üles. Kui keegi usinatest ei avasta sellist tegevust hiljem ning ei anna sellest õppejõule tead, siis on laisk õpilane sisuliselt mitte midagi tehes saavutanud sama tulemuse, kui usinad õpilased. Selline ei ole kindlasti ühegi grupitööna mõeldud ülesande eesmärk ning seepärast loeb autor sellist tegevust ründeks TTÜ veebitestide vastu.



## **6.3 Veebikeskkonna identiteedivargus**

TTÜ veebikeskkondade kontekstis oleks identiteedivarguseks kellegi teise eest veebitesti pahatahtlik sooritamine või omakasu eesmärgil kellegi virtuaalidentiteedi ärakasutamine. Mõlemal juhul on tegu üldiselt lubamatu ligipääsuga seostuvate juhtumitega ning ligipääsuks vajalik info on omandatud ilma identiteedi omanike loata. Sellist rünnakut oleks teoreetiliselt võimalik vältida biomeetriaga seotud pidevate autentimismeetoditega [12].

### **6.3.1 Pahatahtlik veebitesti sooritamine**

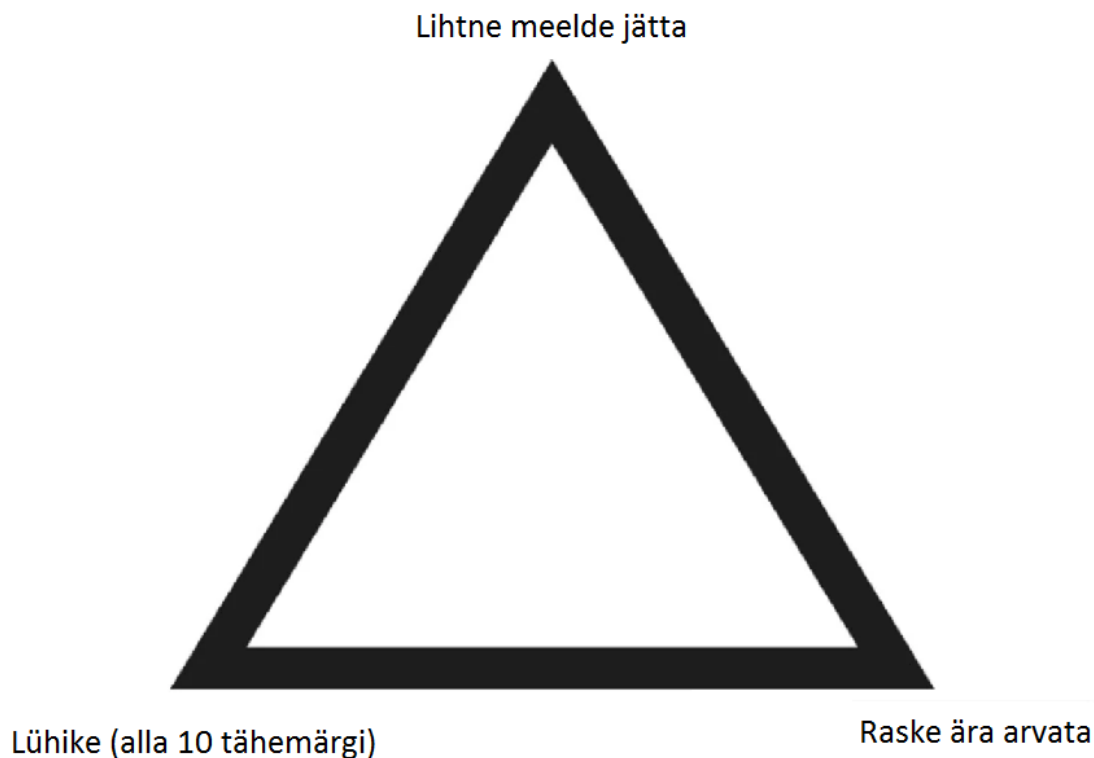
Tihti on ainetes suurt tähtsust omavad testid veebitestide keskkondades sooritatavad ainult ühe korra. Selline veebitestide loomise viis on üsnagi levinud, mispärast on sellekohaste juhtumite teoreetiline tekkimise võimalus suurem, kui arvata võiks. Kui selline juhtum peaks aset leidma, siis on tudengil väga raske tõestada, et tema tõesti ei ole üritanud testi sooritada. Õppejõud võib heas usus lasta õpilasel testi uuesti sooritada, kuid arvan, et selline otsus nõuab palju pimedat usaldust tudengi suunas, mida mitmel õppejõul kindlasti ei ole. Sellisele lahendusele ei aita ka kaasa fakt, et tihti ained, kus ühekordsed veebitestid esinevad, võivadki olla ainult veebipõhised ning õppejõud ja tudeng ei kohtu kunagi. Tähtis on ka märkida, et sellise rünnaku puhul ei pruugi olla ligipääs omandatud ilma identiteedi reaalse omaniku teadmisseta. Tegu võib olla tahtlikult jagatud infoga, mida teine osapool otsustas lihtsalt pahatahtlikult ära kasutada.

## **6.4 Omakasu eesmärgil virtuaalidentiteedi ärakasutamine**

Kellegi virtuaalidentiteedi ärakasutamine omakasu eesmärgil üldiselt väljenduks näiteks õppejõu virtuaalidentiteedist tuleneva ligipääsuga veebitestide keskkonnas testide juures määratud õigete vastuste vaatamist või isegi tulemuste muutmist. Sellise rünnaku puhul võib kindlalt öelda, et ligipääs on omandatud ilma õppejõu loata. Hinnete muutmise rünnakut saab ainult avastada õppejõud omades kuskil tagavara koopiat algsetest hinnetest. Mõlemat rünnakut peaks saama ideeliselt kontrollida logide abil vastava veebitestide keskkonna andmebaasist, seda juhul kui ligipääsemine kontodele salvestatakse logides.

## 7 Viisid virtuaalidentiteedivarguse tõkestamiseks

Enamik veebilehti kasutavad kasutaja identifitseerimiseks kasutajanime ja parooli paari. Et tõkestada identiteedivargust olukorras, kus vajalik info kellegi identiteedi üle võtmiseks koosneb kahest tekstijupist, vastavalt kasutajatunnus ja parool, tuleks tähelepanu pöörata just parooli osale. Seda põhjusel, et kasutajanimede nimekiri on üldjuhul veebilehtedel olemas. Leidub ka lehti, kus nimekirja olemasolu asemel on rakendatud otsinguvormi, mille abil on võimalik kasutajaid otsida.



Joonis 1. Parooli valimise atribuudid

Parooli valimisel tuleks meeles pidada erinevaid aspekte, mida võib lihtsustatult kujutada kolme atribuudina (vaata joonis 1.), millest absoluutselt valida on võimalik ainult kaks. Selline piirang tuleneb loogilisest järeldusest, et miski mis on lihtsasti meelde jäetav ning on lühike, on arvatavasti kergesti arvatav. Sellise loogilise järelduse saab ka teiste paaride valimisega. Näited paaride kohta on toodud tabelis 1.

Reaalses maailmas ei peaks kunagi valima nendest kolmest atribuudist absoluutselt kahte ning neid järgima. Üldjuhul peaks parool tuginema kõigile kolmele omadusele. Kõige tähtsamaks peaks olema ära arvamise raskus, sest see ongi üldine

parooli omamise eesmärk. Kõige rohkem tuleks autori arvates ohverdada parooli lühisust, kui eesmärgiks on teadlikult turvaline parool. Pikema parooli näol on tegemist raskemini meelde jäetava parooliga, kuid on mõisteta, et turvaline parool sellist järeleandmist nõuab.

Tabel 1. Atribuutide valikud ja näited

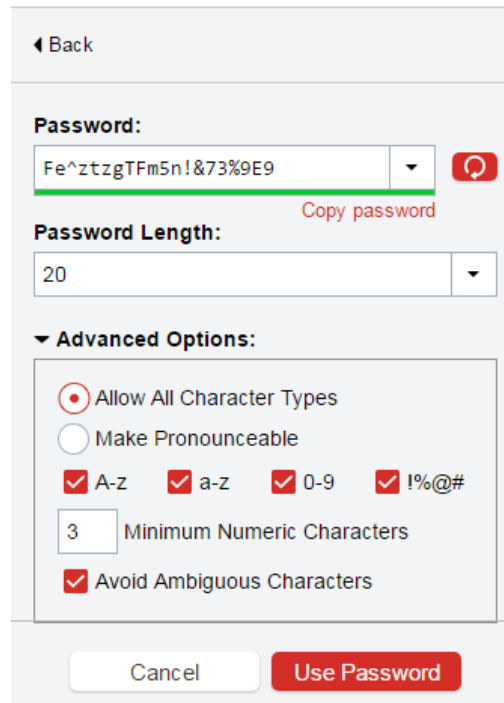
| Lühike | Lihtne meelde jätta | Raskesti arvatav | Näide                      |
|--------|---------------------|------------------|----------------------------|
| JAH    | EI                  | JAH              | 4Rer\$“#gbx’               |
| JAH    | JAH                 | EI               | minuparool                 |
| EI     | JAH                 | JAH              | minumajaonsininejaroheline |

## 7.1 Alternatiivne parooli valimise lahendus

On olemas brauserite juurde käivaid lisasid, mis endast kujutavad paroolihaldureid. Sellist võimalust pakuvad näiteks LastPass [13], Dashlane [14] ja 1Password [15]. Paroolihaldureid saab kasutada kõigi hetkel populaarsete brauseritega. Paroolihaldurid hoiustavad pilveteenuses soolatud räsina kõiki paroole, mille on kasutaja sinna lisanud. Olles paroolihaldurisse sisse loginud ning seejärel liikunud veebilehele, mille kohta oled salvestanud parooli haldurisse, täidab brauser automaatselt kasutajanime ning parooli lahtrid. Paroolihaldurite kasutamiseks on enamjaolt vajalik luua kasutaja, mille kasutajanimeks on e-mail, eeldatavasti paroolihalduri kasutamist sooviva isiku oma. Selle kasutaja parool kujutab endast LastPassi kontekstis ülemparooli, millega pääsed hiljem oma teistele paroolidele ligi, ilma et peaksid paroolihaldurisse lisatud paroole teadma. Tähtis on meeles pidada ainult ühte ülemparooli. Tänu sellele, et meeles on vaja pidada ainult ühte parooli mitme asemel, peaks ülemparooli näol olema tegu millegi turvalisemaga, kui tavalise parooliga.

Lisaks pakuvad paroolihaldurid tihti ka parooli genereerimise võimalust (vaata joonis 2.), kus on võimalik pakutavate parameetrite järgi genereerida suvalist parooli, mille saab peale kasutamist ära salvestada paroolihaldurisse, kust seda võimalik kätte saada ning kasutada ilma et peaks suvaliselt genereeritud parooli meelde jätma. Kuna genereeritavad paroolid on vastavalt valitud parameetritele suvalised, siis on need ka

kohelelt raskesti ära arvatavad, seda muidugi kui suvalise parooli genereerimiseks valitud parameetrid võimaldavad keerulise parooli tekkimist (vaata joonis 2.).



◀ Back

**Password:**

Fe^ztzgTFm5n!&73%9E9

**Password Length:**

20

▼ **Advanced Options:**

Allow All Character Types

Make Pronounceable

A-z  a-z  0-9  !%@#

Minimum Numeric Characters

Avoid Ambiguous Characters

Joonis 2. LastPassi parooli genereerimise kasutajaliides

## 8 Jooksvalt identiteedi kontrollimine

Pidev identifitseerimine on üks potentsiaalne lahendus takistamiseks virtuaalidentiteedivargust. Pideva identifitseerimise näol tuleb tuua arvatavasti ohvride kasutusmugavuse arvelt. See võib väljenduda näiteks pideval parooli uuesti sisestamisel, või muu identiteedi tuvastuseks kasutatava meetodi uuesti läbi tegemine. On räägitud ka identifitseerimismeetoditest, mis ei mõjutaks lõppkasutaja kogemust.

### 8.1 Näotuvastus

Üheks biomeetriliseks tuvastusmeetodiks on potentsiaalselt nägu. Facebooki poolt tehtud projekti DeepFace raames oli nende näotuvastus algoritm 97.25% täpne [16]. 2016 Washingtoni ülikooli poolt tehtud uuringus, kus algandmeteks võeti 690 572 unikaalset isikut, kelle kohta koguti 1 miljon pilti. Kõige täpsem oli 75%-ga Google algoritm FaceNet. [17] Näotuvastuse kasutamise üks eeldus on veebikaamera olemasolu. Seda eeldust täites ning arvestades, et näotuvastusalgoritmid ei ole perfektsed, kuid on piisavalt head, siis on tegu reaalse lahendusega pideva identifitseerimislahenduseni jõudmisel.

### 8.2 Silmad

Silmaiirise tuvastust on kasutatud näiteks filmides kõrgtehnoloogilise identifitseerimismeetodina. Silmaiirisel on 240 võrdluspunkti, mida on viis korda rohkem kui näpujäljel [18], mis teeb silmaiirise palju turvalisemaks, kui seda on näpujalg. Tänapäeval on iirise leidmise ja ära tundmise algoritmid muutunud väga täpseteks. [19] Tehtud analüüs leidis, et nende pakutud algoritm suutis 87% täpsusega leida silmaiirise. Valepositiivseid leidis algoritm 0.007% ja valenegatiivseid 2.4% [19]. Iirise tuvastuse kasutamine laialdasemalt jääb siiski raudvaralise piirangu taha, sest enamikul arvutitel ei ole kaasas infrapuna kaamerat, millega saaks iirist efektiivselt skaneerida. Mitmed uuemad nutiseadmed omavad võimalust kasutada telefoni lukust avamiseks silma iirise tuvastust tänu seadmel asuvale infrapuna andurile [20].

Lisaks on India käsil suurprojekt, mille käigus tahetakse kõikide kodanike iirised ja sõrmejäljed skaneerida süsteemi. Peale skaneerimist väljastatakse isikule Aadhaar kaart, mis käitub kui isikut tõendav dokument, sarnaselt Eestis ID-kaardiga

[21]. Erinevus tuleneb Aadhaar kaardi seotusest selle omaniku biomeetriaga, ID-kaardil selline seos puudub.

### **8.3 Trükkimine**

Trükkimismeetodid on veel üheks biomeetriliseks omaduseks, mille kaudu on potentsiaalselt võimalik identifitseerida klavvivajutusi tegevast isikut. Selle meetodi rakendamiseks mõeldakse erinevate klavvivajutuste vahelist aega ning klahve mida vajutatakse. Suure hulga andmete kogumisega tekivad mustrid, näiteks keegi vajutab 95% juhtudel klahvi „E“ peale klahvi „S“ 0,3 sekundi pärast. Kui järsku peaks selle identiteedi alt esinev isik näiteks vajutama klahvi E peale klahvi „S“ 1 sekundi pärast, siis võiks tekkida kahtlus, et tegu ei pruugi olla enam sama isikuga, kes algselt. [22]

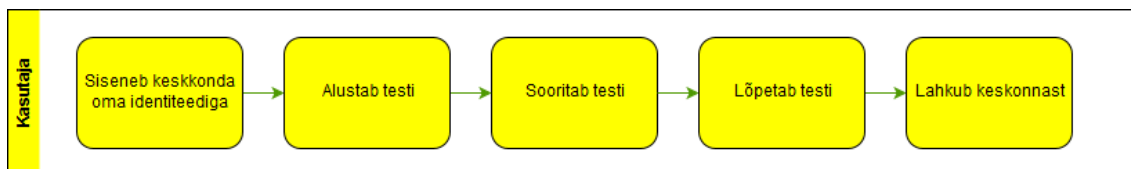
Erinevalt iirise ja näotuvastusest on tegu käitumisharjumustega seotud biomeetrilise omadusega. Trükkimise puhul on tegu siiski teoreetiliselt täpse identifitseerimismeetodiga, sest trükkimisharjumused kujunevad pika aja jooksul ja on pikema aja jooksul selgesti eristatavad üksteisest. Seda tuvastusmeetodit peetakse kõige kasutajasõbralikumaks, sest meetod ei nõuaks kasutajalt lisategevusi, erinevalt iirise skaneerimisest ning näotuvastusest. Allikas [22] tehtud töö kohaselt oli nende poolne veebilahendus keskmiselt 99% täpne isiku tuvastamises parooli kirjutamisel. Lisaks oleks võimalik allika [23] kohaselt kasutada trükkimise kohase info kogumist kasutada hiljem teksti autori identifitseerimiseks.

#### **8.3.1 Nutiseadmes trükkimine**

Nutiseadmetes käib trükkimine üldjuhul puutetundliku ekraani abil. Sellisel juhul ei ole trükkimismeetodite analüüsimine väga usaldusväärne lahendus, sest erinevatel nutiseadmetel on erinevad klavvipaigutused ning erinevad nupusuurused mis kõik mõjutavad kirjutamise täpsust ja kiirust. Selle eelduse põhjal saaks järeldada, et andmete kogumise tulemusel oleks ühe isiku harjumuste kaardistamine süsteemil väga keeruline. Harjumuste ebatäpne kaardistamine tekitab suure võimaluse, et identifitseerimismeetod võib anda valepositiivseid tulemusi, ehk valesti tuvastada võõra isiku. Selle info põhjal arvab autor, et trükkimismeetodite analüüs ja kasutus identifitseerimismeetodina võiks olla lahenduseks ainult arvuti kasutamisega seoses.

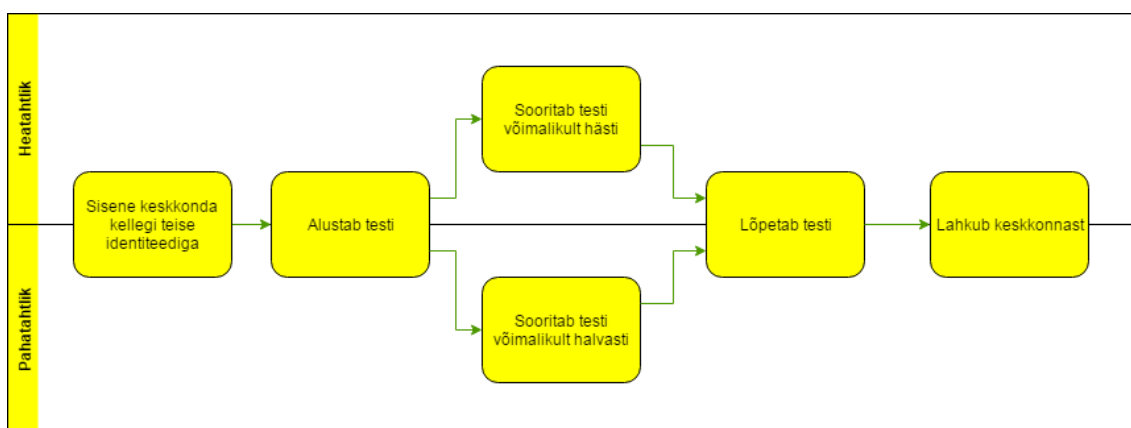
## 9 Virtuaalidentiteedi ründe analüüs ning kaitse võimalused veebitestide keskkonnas

### 9.1 Tavalise kasutaja kasutusjuht



Joonis 3. Kasutaja kulg testikeskkonnas

Tavaline kasutaja, kes siseneb veebitestide keskkonda testi sooritamise eesmärgil läbib joonisel 3 kujutatud teekonda keskkonnas. Juhul kui on tegu virtuaalidentiteedivargusega, mille alla kuulub ka kellegi teise isiku kasutaja alt testide tegemine, siis saab jaotada kasutusjuhu pahatahtlikuks ning heatahtlikuks. (vaata joonis 4.)



Joonis 4. Hea- ja pahatahtliku võõra identiteedi kasutaja kulg testikeskkonnas.

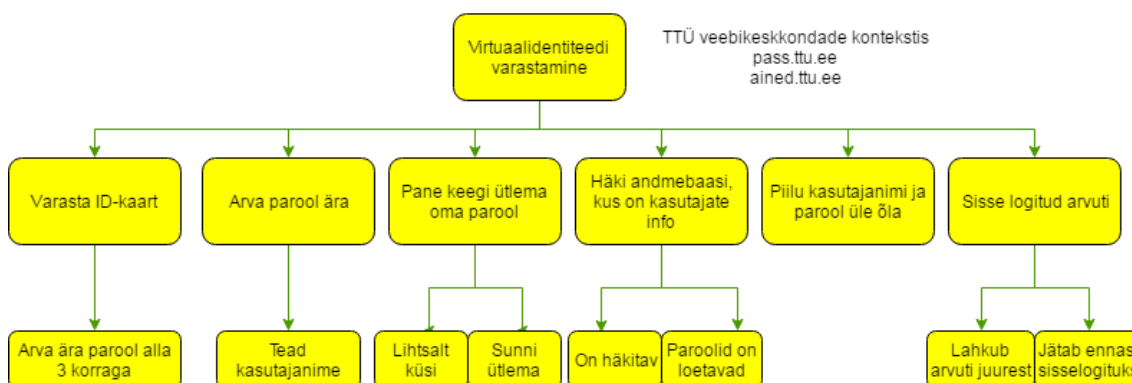
Ideeliselt sooritab heatahtlik võõra virtuaalidentiteedi kasutaja vastava identiteediga testi võimalikult hästi, seda kas heast tahtest või omakasu eesmärgil. Omakasuks peaks siinkohal mingisuguse tasu eest kellegi testi tegemist. Pahatahtlik kasutaja on ideeliselt võimaldanud endale ligipääsu kellegi teise virtuaalidentiteedile mingisuguse virtuaalidentiteedi vastase ründe abil, millega omandas vajaliku info. Sellisel juhul on antud joonise 4 põhjal eesmärgiks test võimalikult halvasti sooritada, seda kas halvast tahtest või jällegi omakasu eesmärgil. Omakasuks peaks siinkohal

kellegi soovil tahtlikult kellegi kolmanda isiku nimel testi halvasti sooritamist mingisuguse kasu eest.

Sellise olukorra vältimiseks on vajalik tuvastada antud kasutusjuhu nõrgad kohad, neid analüüsida ning leida potentsiaalseid lahendusi nende nõrkade kohtade rünnakute tõkestamiseks. Antud juhul on kõige nõrgemaks kohaks keskkonda sisenemine, sest peale algset identifitseerimist ei veenduta, kas keskkonda kasutatav isik on tõesti see, kelleks ta ennast esitleb.

## 9.2 Ründe analüüs

Potentsiaalsete rünnete kirjeldamine üldiselt on läbinud läbi aegade mitmeid iteratsioone. Hetkel on üheks väga levinud meetodiks lihtsalt mõistetavate ründepeude kasutamine. [24] Selle selgitusmeetodiga saab luua illustratiivse joonise, millelt on näha potentsiaalse ründe erinevad võimalused. (vaata joonis 5.)



Joonis 5. Virtuaalidentiteedi varastamise ründepuu.

Kõik rünnete võimalused ei ole kindlasti võrdsed. Võiks väita, et mõned on neist praktiliselt võimatud. Järgnevalt analüüsin kõiki joonisel 5 asuvaid võimalusi eraldi ning klassifitseerin rünned keerukuse järgi lihtsaks, keeruliseks ja väga keeruliseks. Tegu on subjektiivse hinnanguga.

### 9.2.1 Varasta ID-kaart

ID-kaardi varastamise abil virtualidentiteedi varastamiseks on vaja peale füüsilise ID-kaardi ka kaardi PIN1-te, kui on soov mingisugusesse keskkonda siseneda ning PIN2-te kui on soov midagi allkirjastada. Antud kontekstis kasutatakse ID-kaarti



ainult identifitseerimiseks, ehk teisisõnu keskkonda sisenemiseks. Antud ründe korral tuleb pahalasel ära arvata PIN1. PIN1 puhul on tegu nelja kohalise numbriga, mis on ID-kaardi saamisel suletud ümbrikus. PIN1 sisestamiseks on kolm katset. Peale kolmandat katset ID-kaart suletakse ning selle avamiseks peab pöörduma Politsei- ja Piirivalveameti kontorisse. Tõenäosus, et kolme korraga ära arvata nelja kohaline kood on 0,03% ( $3 * (1 / 10000) * 100\%$ ). Eelnevast faktist tulenevalt on tegu keerulise ründega, sest ID-kaarti ennast varastada ei ole põhimõtteliselt keeruline, kuid PIN1 ära arvamine on.

### **9.2.2 Arva parool ära**

Parooli ära arvamine suvaliselt proovides eeldab kasutajanime varasemat teadmist. Samuti on realistlikult selle ründe eelduseks, et keskkond laseb sisestada lõpmatul arvul kordi parooli. TTÜ IT ained keskkonna sisselogimise lehel on katsete arv piiratud. See teeb parooli edukalt ära arvamise väga ebatõenäoliseks, sest UNI-ID parool peab olema vähemalt 8 tähemärki pikk ning ainult 8 tähemärki pikki paroole on ligikaudu 3 000 000 000 000 000 000 ehk 3 kvadriljonit [25]. See teeb iga katse tõenäosuseks 0,000000000000003%. Eelnev number ei arvesta pikemaid paroole kui 8 tähemärki. Selle teadmise tõttu on suvaliselt kellegi parooli ära arvamine väga ebatõenäoline. Eelneva fakti tõttu on ründe edukuse tõenäosus väga madal mis teeb ründe väga keeruliseks.

### **9.2.3 Pane keegi ütlema oma parool**

Antud ründel on kaks võimalust, kas isik ütleb oma parooli lihtsalt küsides, või seda on vaja kuidagi isikult kätte saada. Parooli lihtsalt küsimise teel omandamist võiks tõlgendada ka tahtlikult parooli andmisena, ehk teisisõnu vastavasse kasutajasse sisenemise loa andmisena. On täiesti realistlik, et ründaja võiks seda vastavalt tõlgendada ning süü tuvastamine oleks hiljem keeruline, sest väga põhimõttelisel tasemel muutub selline süüdistus sõna-sõna vastu vaidluseks.

Sunniviisiliselt parooli omandamine võib endaga kaasa tuua sekeldusi seadusega, sest teoreetiliselt katab sunniviisiline parooli, ehk info, saamine ka piinamisvõtteid ning need on vastuolus Eestis kehtiva karistusseadustikuga, näiteks §120 - §122 [3].

Puht põhimõtteliselt on tegu lihtsa rünnakuga, sest esineb võimalus, et kasutaja lihtsalt ütlebki oma parooli. Samas mingisuguse sunniviisilise meetodiga parooli kättesaamine on väga ebaeetiline, kuid võiks eeldada, et sellel viisil parooli kätte saamine on arvatavasti üsnagi edukas. Nende eelduste järgi klassifitseeriks autor selle ründe lihtsaks.

#### **9.2.4 Häki andmebaasi, kus on kasutajate info**

Andmebaasist kasutajainfo omandamine oleks süsteemselt kõige otsesem viis kellegi virtuaalidentiteedi omandamiseks. Endale võõrasse andmebaasi ligipääsu võimaldamine läheks vastuollu Eestis Karistusseadustiku §217 lg 1 sättega ning sellise teo eest karistatakse rahalise karistuse või kuni kolmeaastase vangistusega [3]. Andmebaasist kasutajainfo eraldamine eeldab, et andmebaasis asuvad kasutajanimed ja paroolid lihttekstina. Selline paroolide salvestamise viis on väga ebaturvaline, sest ükskõik kes võib ligipääsu omades lihtsalt lugeda salvestatud paroole. Pigem soovitatakse salvestada paroole krüpteerituna.

Lisaks krüpteeringule soovitatakse veel paroole soolata, ehk lisada parooli krüpteerimisele juurde veel suvaliselt genereeritud tekstijupp, mis teeb krüpteerimise tulemusel saadud segase tekstijupi veelgi äraarvamatuks. [26] Krüpteeritud ja soolatud paroole saab potentsiaalselt kätte ainult suvaliselt proovimise teel, ehk siis proovitakse erinevaid tähekombinatsioone koos soolaga läbi süsteemis kasutusel olnud krüpteerimise algoritmi ja loodetakse tulemuseks saada samasugune tekstijupp nagu andmebaasis salvestatud oli. Selline lähenemine eeldab, et kuidagi on varasemalt saavutatud ligipääs andmebaasile, kust on eraldatud läbi krüpteerimise ja soolamise tekkinud tekstijupp ning soola väärtus ise.

Eeldades, et paroolid on andmebaasis salvestatud turvaliselt, siis on tegu väga keerulise ründega. Ründe edukus sõltub tugevalt andmebaasi turvalisusest ning hinnang lähtub populaarsete turvanõuete järgimisega tegeleva andmebaasi vaatepunktist.

#### **9.2.5 Piilu kasutajanimi ja parool üle õla**

Antud ründe põhjal on tegu pahatahtlikult kasutaja järel nuhkimisega, mille tulemusena omandatakse info kasutaja virtuaalidentiteediga seostuva kasutajanime ja parooli kohta. Seda infot kasutaks pahatahtlik isik hiljem ära ründe ohvri virtuaalidentiteedile ligipääsemiseks. Sellisele rünnakule ei ole peale enda valvsuse

otseseid kaitsemeetmeid. Kaudselt võib kaitsemeetmeteks pidada parooli kiiret trükkimist, et ründajal oleks raske seda jäädvustada. Eelnevat kaitsemeetodit võiks kombineerida parooli pikkuse ja raskusega.

Sellest, et meetod ei nõua põhimõtteliselt mingisugust ettevalmistust ega kokkupuudet klassifitseeriks autor ründe lihtsaks.

### **9.2.6 Sisse logitud arvuti**

Arvuti tagant lahkudes arvuti sisselogituks jätmine on üks potentsiaalseid ründeviise kellegi virtuaalidentiteedi suunas. Tegu on kõige vähem ründaja poolset pingutust nõudva ründega antud kontekstis, sest praktiliselt ei ole ründajal vaja mitte midagi teha. Sellise ründe tõkestamine on ainult kasutaja enda kätes. Kuivõrd selline rünne on ohvri kätest väljas alates toimumise hetkest, siis on mõned süsteemid rakendanud endas viise selle vältimiseks. Näiteks on mõnedele veebilehtedele lisatud sessiooni aegumise aeg. See kujutab endast automaatset väljalogimist mingisuguse aja ebaaktiivuse järel. Kui ründaja on selline, kes jõuab arvutisse enne selle aja möödumist, siis ei ole ka sellest kaitsemehhanismist abi.

Sarnaselt eelnevas punktis mainitud ründega ei nõua rünne mingisugust ettevalmistust ega otsest kokkupuudet, tegu on lihtsalt võimaluse tekkimisega ning selle tõttu on ka sisse logitud arvuti ründe korras tegu, autori arvates, lihtsa ründega.

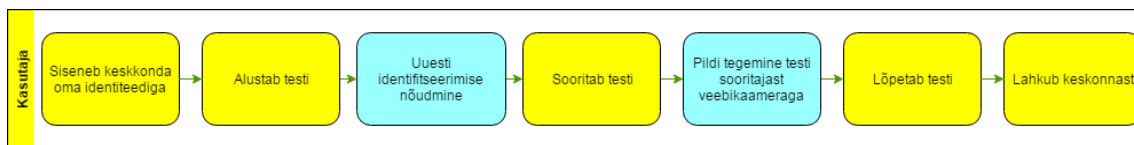
## **9.3 Kaitse virtuaalidentiteedi varastamise ründele**

Virtuaalidentiteedi varastamise ründele on üldiselt mitmeid vastumeetmeid. Oma identiteedi kaitsmist peaks alustama tugeva parooli valimisest, oma parooli mitte korduv kasutamisest, teistele mitte jagamisest ning teiste ees selle mitte sisestamisega. Samuti ei tohiks kindlasti jätta oma arvutit sisselogituks peale enda lahkumist. Nende lihtsate meetmete kasutamine hoiab vaieldamatult ära paljud potentsiaalsed ründed.

Ründe edukust vähendaks ka kindlasti uuesti identifitseerimine peale testi alustamist (vaata joonist 6), et veenduda kas tegu on tõesti vastava identiteedi omanikuga. Uuesti identifitseerimisel peaks olema nõutud algsest identifitseerimisest erineva identifitseerimismeetodi kasutamist. Vastasel juhul võib ründaja kasutada algset informatsiooni lihtsalt uuesti. Uuesti identifitseerimisel oleks hea, kui kasutataks identifitseerimiseks näiteks ID-kaarti. See muudaks identifitseerimise sisuliselt

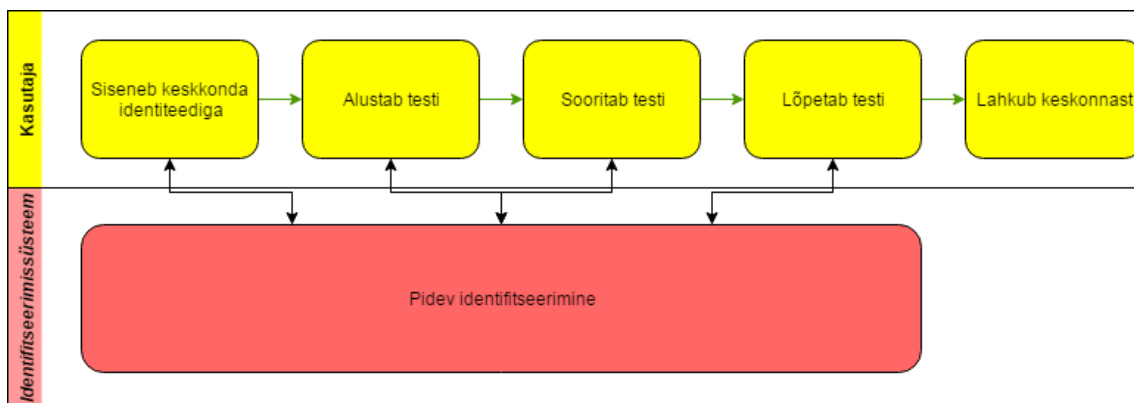
kahefaktoriliseks, algne sisse logimine käiks kasutajanime ja parooli abil, ehk siis miski mida tead ning teine identifitseerimine on ID-kaardi abil, miski mida omad.

Kui rünne kellegi virtuaalidentiteedi vastu peaks õnnestuma, siis on vajalik omada võimalust seda tõendada ning võimaluse korral ründaja tabada. Seda eesmärki saab kaudselt täita, kui nõuda testi lõpetamisel veebikaameraga tehtud pilti arvuti taga istuvast isikust (vaata joonist 6.). Kui isik on see, kelleks ta ennast väidab, siis ei ole mingisugust probleemi. Kui hiljem peaks tekkima pretensioone kellegi poolt, kes väidab, et tema pole testi sooritanud, siis saab kasutada testi lõpetamiseks nõutud pilti kui verifitseerimismeetodit, et veenduda kes tegi testi. Kui testi tegija ei olnud tõesti identiteedi omanik, siis võiks ideeliselt lubada testi uuesti sooritada. Sellisel juhul on pahatahtliku ründaja rünne tehniliselt küll õnnestunud, kuid praktiliselt mitte, sest rünnatav isik ei kaotanud otseselt midagi peale oma aja.



Joonis 6. Kasutaja kulg turvalisemas testikeskkonnas.

## 9.4 Virtuaalidentiteedi varastamise ründe tuvastamine



Joonis 7. Kasutaja kulg identifitseerimissüsteemiga keskkonnas.

Virtuaalidentiteedi ründe tuvastamiseks oleks vajalik kontrollida peale esialgset identifitseerimist ja autentimist keskkonnas liikudes pidevalt identiteediga seotud parameetreid ning võrrelda neid kasutamisel tekkivate metaandmetega. Seda pidevat kontrollimist võiks teostada keskkonda liidestatud identifitseerimissüsteem, mis

keskkonnas toiminguid tehes jälgiks kasutaja tegevust ning võrdleks seda identiteediga seotud andmetega.

#### **9.4.1 Klahvivajutuste jälgimine**

Identifitseerimissüsteemil oleks vaja klahvivajutuste jälgimiseks ligipääsu vastavale infole. Samuti oleks vajalik algne testandmestik millega võrrelda. Ideeliselt sobiks selliste andmete kogumiseks näiteks identiteedi loomisel mingisugune trükkimistest, millega kaardistataks identiteediga seotud üldised trükkimisharjumused. Süsteem iseenesest peaks olema piisavalt optimeeritud ja võimekas reaalajas nende andmete võrdluseks ning peale testi ka nende salvestamiseks, et oleks võimalik analüüsida ja võrrelda teksti terviklikke kirjutamise metaandmeid identiteediga seotud üldiste harjumustega, et tuvastada kas teksti autor oli ikka vastav identiteet [23]. Seda identifitseerimismeetodit võiks identifitseerimissüsteem rakendada igas keskkonna punktis, kus on vajalik trükkimine.

Selline identifitseerimismeetod ei mõjutaks kasutajat absoluutselt, sest tegu on taustal toimuva protsessiga, mille tulemused väljenduksid vaid juhul, kui on tuvastatud potentsiaalne rünne. Ründe potentsiaalse tuvastuse korral nõutaks kasutajal end autentida algsest autentimismeetodist erineval viisil, sest vastasel juhul võiks algsel autentimisel kasutatud infot taaskasutada. Juhul, kui autentimine õnnestub, siis võiks süsteem paluda kasutajal taas läbida identiteedi loomisel nõutud trükkimistest, et värskendada identiteediga seotud trükkimisharjumusi. Selline nõue tuleneb eeldusest, et süsteem tuvastaks valepositiivsena isiku sellisel juhul, kui tema trükkimisharjumused on drastiliselt muutunud võrreldes identiteedi loomisel läbitud testist saadud andmetega.

#### **9.4.2 Näotuvastus**

Identifitseerimissüsteem saaks ja võiks kasutada pidevat näotuvastust, kui identifitseerimismeetodit. Selle meetodi rakendamine nõuaks kasutajalt veebikaamera olemasolu ning süsteemilt märgatavat jõudlust, et reaalajas seda läbi viia. Facebooki projekti DeepFace täpsus oli 97,25% [16], mida peaks autor piisavalt täpseks, et rakendada näotuvastust ka pideva identifitseerimismeetodina. Võiks vaielda, et 97,25% täpsus saavutati ainult piltide võrdlusega, kuid videot võibki tõlgendada kui järjest käivaid pilte. Selle loogika põhjal ei oleks pideval näotuvastusel ja ühekordsel näotuvastusel otseseid erinevusi, mis takistaks meetodi rakendamist.

Selline identifitseerimismeetod ei mõjutaks kasutajat absoluutselt, sest tegu oleks taustal toimuva protsessiga. Kasutajalt oleks nõutud, eelmainitult, veebikaamera ning nõusolek selle kasutamiseks keskkonna poolt.

Süsteem peaks ka olema võimeline arvestama pause ning võimalust, et korraks võibki teine isik sattuda testi käigus arvuti taha ja seda mitte testi tegemise eesmärgil. Täpsed parameetrid näotuvastuse algoritmile ning vastavad reeglid tuleks vastava programmi või süsteemi arendajal täpsustada, kuid see ei ole praeguse töö skoobis.

### **9.4.3 Korduv autentimine**

Süsteem peaks mingisuguse süsteemi väljatöötaja poolt määratud aja tagant nõudma kasutajalt uuesti autentimist. See kujutaks endast näiteks uuesti parooli sisestamist või mingil muul viisil identiteedi tõestamist. Kujutlikult võib seda tõlgendada kui uuesti sisselogimist. Selline identifitseerimissüsteemi funktsionaalsus vähendaks arvuti tagant lahkumisel tekkiva rünnaku riski. Sellise olukorra puhul ei pruugi ründaja omada identiteediga seotud salasõnade või muude parameetrite kohta mingisugust infot, mispärast ei oskaks ründaja korduv autentimise nõude korral midagi ette võtta ning rünne teoreetiliselt nurjuks.

Korduva autentimise nõudmine oleks kasutajale potentsiaalselt ebamugav, sest see võib hetkeliselt katkestada olnud mõttekäigu või üleüldise vaimse töö hoo. Kuigi võiks vaielda, et identiteedi turvalisuse tagamine on tähtsam kui hetkeline katkestus, on siiski tegu subjektiivse teemaga, mispärast on ühest raudset vastust praktiliselt võimatu välja käia.

Antud kaitsemehhanismi kasutavad praegusel hetkel näiteks Eestis panganduses, kus nõutakse maksete tegemisel uuesti autentimist, seda siis ID-kaardi PIN2 nõudmise, või paroolikaardilt parooli sisestamise läbi. Sellest, et antud meetod on kasutusel ka igapäevaelus kriitilistes valdkondades, võiks järeldada, et tegu on hea ning vajaliku meetmega identiteedi turvalisuse tagamisel ning kasutajamugavuse mingil määral ohverdus on igati õigustatud.

### **9.4.4 Silmairise skaneerimine**

Silmairise identifitseerimismeetodina kasutamine sobiks nii algseks identifitseerimiseks, kui aeg-ajalt uuesti identifitseerimiseks, sest tegi on igale inimesele

kuuluva unikaalse omadusega. Silmaiirise skaneeringute puhul on valepositiivse tulemuse võimalus  $1 / 1\,200\,000$  [20] ning valenegatiivse tulemuse võimalus „*very close to zero*“ [20], ehk nullilähedane.

Tegu oleks kindlasti, kasutaja poolt vaadatuna, pigem ebamugava lahendusena, sest silmaiirise skaneerimiseks on vaja spetsiifiliselt olla kaamera ees nii, et silmad oleks selgelt kaamerale näha ning ruumis oleks piisavalt valgust. Kuigi silmaiirise leidmine ja pildi tegemine on muutunud väga täpseks [19] oleks sellise identifitseerimismeetodi kasutamine kasutaja jaoks siiski ebamugav. On vaieldamatu, et tegu oleks väga turvalise identifitseerimismeetodiga, sest tegu on igale inimesele kuuluva unikaalse omadusega, kuid olukordi, kus antud identifitseerimismeetodi kasutamine võib olla raskendatud, või isegi võimatu, võib olla takistuseks sellise meetodi realiseerimise juures.

Selle meetodi rakendamiseks identifitseerimissüsteemi osana tuleks sügavalt läbianaalüüsida täpsed parameetrid, mis on vajalikud meetodi edukaks kasutamiseks ning kaardistada nendega seotud probleemid, kuid see on antud töö skoobist väljas.

## 10 Kokkuvõte

Töös tutvustati erinevaid virtuaalidentiteedi kasutuskohti TTÜ veebikeskkondade kontekstis ning nendega seostuvaid potentsiaalseid ründeid. Lisaks kaardistati virtuaalidentiteedivargusega seotud rünne ning töö tulemusena pakutakse lahendusena virtuaalidentiteedi vastu suunatud rünnakutele pidevat identifitseerimissüsteemi, mis jälgiks taustal kasutaja tegevust ning nõuaks aeg-ajalt korduv autentimist.

Selline süsteem vähendaks potentsiaalset rünnete riski ning looks teoreetilise võimaluse peale rünnaku toimumist seda tõendada. Need kaks omadust oleks nii süsteemi kasutajate kui ka haldajate poolt kindlasti soovitud. Tulevikus oleks vajalik täpsemad parameetrid identifitseerimisele kaardistada ning vastav süsteem välja arendada. Töö loob tulevikus sellise identifitseerimissüsteemi väljatöötamiseks head eeldused tehes ära märgatava osa analüüsist ning kaardistades probleemi, mida süsteem lahendada peaks.



## Kasutatud kirjandus

- [1] „Tor Project: Overview,“ [Võrgumaterjal]. Available: <https://www.torproject.org/about/overview.html.en>. [Kasutatud 10 4 2017].
- [2] „Digiallkirjastamine > Mida saab ID-kaardiga teha > ID-kaart ja Digi-ID > ID-kaart > ID.ee,“ SK, [Võrgumaterjal]. Available: <http://www.id.ee/?lang=et>. [Kasutatud 12 4 2017].
- [3] Riigikogu, „Karistusseadustik - Riigi Teataja,“ 10 1 2017. [Võrgumaterjal]. Available: <https://www.riigiteataja.ee/akt/184411?leiaKehtiv>. [Kasutatud 10 4 2017].
- [4] „Õppeinfosüsteem,“ TTÜ, [Võrgumaterjal]. Available: [https://ois.ttu.ee/pls/portal/ois2.ois\\_public.main](https://ois.ttu.ee/pls/portal/ois2.ois_public.main). [Kasutatud 10 4 2017].
- [5] „Home (Front Page),“ TTÜ, [Võrgumaterjal]. Available: [ois2.ttu.ee](http://ois2.ttu.ee). [Kasutatud 10 4 2017].
- [6] Microsoft, [Võrgumaterjal]. Available: <http://mail.ttu.ee>. [Kasutatud 11 4 2017].
- [7] „TTÜ IT AINED,“ TTÜ, [Võrgumaterjal]. Available: <https://ained.ttu.ee/>. [Kasutatud 12 4 2017].
- [8] „pass.ttu.ee,“ TTÜ, [Võrgumaterjal]. Available: <https://pass.ttu.ee/>. [Kasutatud 10 4 2017].
- [9] „#HITSA,“ HITSA, [Võrgumaterjal]. Available: <http://www.hitsa.ee/sihtasutusest/pohikiri>. [Kasutatud 11 4 2017].
- [10] „TAAT,“ ETAIS, [Võrgumaterjal]. Available: <http://taat.edu.ee/main/>. [Kasutatud 11 4 2017].
- [11] „TTÜ TARKVARATEADUSE INSTITUUT,“ [Võrgumaterjal]. Available: [http://maurus.ttu.ee/yld\\_index.php](http://maurus.ttu.ee/yld_index.php). [Kasutatud 11 4 2017].
- [12] L. M. A. C. Francesco Brancati, „Continuous and Transparent User Identity Verification for Secure Internet Services,“ *IEEE Transactions on Dependable and Secure Computing*, kd. 12, nr 3, pp. 270-283, 2015.
- [13] „How It works,“ LastPass, [Võrgumaterjal]. Available: <https://www.lastpass.com/how-it-works> LastPass. [Kasutatud 10 4 2017].
- [14] „Never forget another password | Dashlane,“ [Võrgumaterjal]. Available: <https://www.dashlane.com/>. [Kasutatud 10 4 2017].
- [15] „1Password,“ [Võrgumaterjal]. Available: <https://1password.com/>. [Kasutatud 10 4 2017].
- [16] J. Lowensohn, „Facebook's working on facial verification that's 'nearing human-level performance' - The Verge,“ The Verge, 17 3 2014. [Võrgumaterjal]. Available: <https://www.theverge.com/2014/3/17/5518808/facebooks-working-on-facial-verification-thats-nearing-human-levels>. [Kasutatud 17 4 2017].
- [17] J. Langston, „How well do facial recognition algorithms cope with a million

- strangers? | UW Today,“ University of Washington, 23 6 2016. [Võrgumaterjal]. Available: <http://www.washington.edu/news/2016/06/23/how-well-do-facial-recognition-algorithms-cope-with-a-million-strangers/>. [Kasutatud 17 4 2017].
- [18] C. Woodford, „How do iris scans work? - Explain that Stuff,“ Explain that Stuff, 5 7 2016. [Võrgumaterjal]. Available: <http://www.explainthatstuff.com/how-iris-scans-work.html>. [Kasutatud 13 5 2017].
- [19] E. M. F. M. F. E. A. E.-S. A. M. Naglaa F. Solimana, „Efficient iris localization and recognition,“ *Optik - International Journal for Light and Electron Optics*, kd. 140, pp. 469-475, 2017.
- [20] L. Wood, „How it works: Iris scanning improves smartphone security | Computerworld,“ 8 9 2016. [Võrgumaterjal]. Available: <http://www.computerworld.com/article/3113028/mobile-security/how-it-works-iris-scanning-improves-smartphone-security.html>. [Kasutatud 17 4 2017].
- [21] R. D. A. C. Shriya Jain, „Biometrics: Human Body as a Password,“ %1 *National Conference on Emerging Trends in Information Technology Cyber Security: Contemporary Threats and Solutions*, 2016.
- [22] C. H. D. H. H. H.-I. K. Sungzoon Cho, „Web-Based Keystroke Dynamics Identity Verification Using Neural Network,“ *Journal of Organizational Computing and Electronic Commerce*, kd. 10, nr 4, pp. 295-307, 2000.
- [23] J. C. S. S.-H. C. John V. Monaco, „Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works,“ %1 *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, VA, USA, 2013.
- [24] B. Schneier, „Academic: Attack Trees - Schneier on Security,“ 1999. [Võrgumaterjal]. Available: [https://www.schneier.com/academic/archives/1999/12/attack\\_trees.html](https://www.schneier.com/academic/archives/1999/12/attack_trees.html). [Kasutatud 10 4 2017].
- [25] „combinatorics - How many possible combination in 8 character password? - Mathematics Stack Exchange,“ StackExchange, 4 2014. [Võrgumaterjal]. Available: <https://math.stackexchange.com/questions/739874/how-many-possible-combinations-in-8-character-password>. [Kasutatud 11 4 2017].
- [26] P. Ducklin, „Serious Security: How to store your users' passwords safely - Naked Security,“ Naked Security, 20 10 2013. [Võrgumaterjal]. Available: <https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/>. [Kasutatud 11 4 2017].