|  |  |
| --- | --- |
| tallinna tehnikaülikool | |
| Infotehnoloogia teaduskond | |
| Tarkvarateaduse instituut | |
|  | |
| Eva Maria Veitmaa 155408IAPB | |
| Kasutaja pidevautentimine Ja PETMISE VÄHENDAMINE VEEBITESTIDES Tallinna Tehnikaülikooli küberkaitse magistriprogrammi sisseastumisTESTI näitel | |
| Bakalaureusetöö | |
| Juhendaja: | Sten Mäses |
|  | MSc |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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: Eva Maria Veitmaa

Annotatsioon

Lõputöö on kirjutatud keeles ning sisaldab teksti leheküljel, peatükki, joonist, tabelit.

Abstract

The thesis is in and contains pages of text, chapters, figures, tables.

Lühendite ja mõistete sõnastik

|  |  |
| --- | --- |
| DevOps | „Koostööd soodustav kultuuriline ja operatiivne mudel, mis tagab IT suure jõudluse ärieesmärkide saavutamiseks.“ [1] |
| Buutima | *To boot*. Alglaadima. „Operatsioonisüsteemi arvuti põhimälusse laadima ja käivitama.“ [2] |
| RAM-ketas | Kirjutatav ketas [2] |
| Brauser | Veebilehitseja, veebisirvija, HTML-dokumentide lugemist võimaldav programm [2] |
| IP-aadress | Internetiaadress, võrgus asuva arvuti või muu seadme identifikaator [2] |
| LMS | *Learning management system*, veebipõhine õppekeskkond, õppeinfosüsteem?. Keskkond, mis võimaldab hallata veebipõhiseid kursuseid, õppematerjale, õppureid ja tulemusi. [3] |
| LTI | *Learning Tools Interoperability*, IMS Global Learning Consortiumi standard õppekeskkondade ja väliste rakenduste ning vahendite ühendamiseks [4] |
| MOOC | *Massive open online course*, vaba juurdepääsuga e-kursus, tasuta veebipõhine kursus [5], [6] |
| LFW | *Labeled Faces in the Wild*, enamasti professionaalsete fotograafide poolt pildistatud kuulsuste fotode andmebaas [7] |
| Funktsiooniklahv | *Function key*. „Kuum klahv“. Spetsiaalset ülesannet täitvad klahvid arvutiklaviatuuril (F1 kuni F12) [2] |
| Spektroskoopia | Aine ja kiirguse interaktsiooni (neeldumine, emissioon, hajumine) uuriv teadusharu [8], [9] |
| Elektroentsefalograafia (EEG) | Ajutegevuse mõõtmine, peaaju bioelektrilise aktiivsuse registreerimine läbi naha, kolju ja ajukestade [8], [10], [11] |
| Elektrokardiograafia (EKG) | Südame elektrilise aktiivuse mõõtmine [12], [13], [11] |
| EER | *Equal error rate*, veamäär[12]. Olukord, mil valepositiivsete ja valenegatiivsete väärtuste esinemine on võrdne [14]. |
| Variisik | Isik, kelle nime all tegutseb keegi teine [15]. Matkimis- ehk kehastusrünnaku ehk identiteedi jagamise läbiviija. Isik A, kes väidab end olevat isik B. |
| Matkimisrünnak, kehastusrünnak | Isiku esinemine kellegi teisena, identiteedi jagamine [16]. Isik A väidab end olevat isik B. |
| NIR | *Near infrared*, lähi-infrapunane (valgus) [17], [18] |

Sisukord

[2.1 10](#_Toc508364831)

[3.1 Kontrollitud ruum 11](#_Toc508364832)

[3.2 Isiku pidev autentimine 12](#_Toc508364833)

[3.2.1 Näotuvastus 13](#_Toc508364834)

[3.2.2 Hääletuvastus 16](#_Toc508364835)

[3.2.3 Iris scan 16](#_Toc508364836)

[3.2.4 Trükkimisstiil, klahvivajutuse dünaamika, kirjutamisprotsessi dünaamika 16](#_Toc508364837)

[3.2.5 Hiire kasutusviis 19](#_Toc508364838)

[3.2.6 Hiire abil autentimine 20](#_Toc508364839)

[3.2.7 Kergbiomeetria (soft biometrics) 21](#_Toc508364840)

[3.2.8 Muu 21](#_Toc508364841)

[3.3 Silmade liikumise ja fookuspunkti jälgimine 22](#_Toc508364842)

[3.4 Ekraanipildi jälgimine 25](#_Toc508364843)

[3.5 Välise lisaekraani keelamine 25](#_Toc508364844)

[3.6 Väliste rakenduste keelamine 25](#_Toc508364845)

[3.7 Ruumi helianalüüs 25](#_Toc508364846)

[3.8 Ruumi pildianalüüs 25](#_Toc508364847)

[3.9 Muu 25](#_Toc508364848)

[4.1 Talview - Remote Proctor/Proview 28](#_Toc508364849)

[4.2 Software Secure - Remote Proctor PRO 29](#_Toc508364850)

[4.3 PSI - Remote Proctor Now 30](#_Toc508364851)

[4.4 Pearson VUE 31](#_Toc508364852)

Jooniste loetelu

No table of figures entries found.

Tabelite loetelu

# Sissejuhatus

# Tallinna Tehnikaülikooli küberkaitse õppekava

Alates 2009. aastast pakub Tallinna Tehnikaülikool tudengitele võimalust õppida küberkaitse magistriõppes [19]. Käesoleva õppekavaversiooni kood on IVCM09/18, maht 120 EAP-d jaotatuna nominaalõppeaja nelja semestri peale ning seda pakutakse koostöös Tartu Ülikooliga [20]. Õppetöö toimub inglise keeles ning juurdepääsu tingimusteks on muuhulgas varasem kõrgharidus või töökogemus info- ja kommunikatsioonitehnoloogia valdkonnas.

Õppekava eesmärgiks on valmistada tudengeid ette süvaõppeks küberkaitse, digitaalse ekspertiisi või krüptograafia peaerialal ning arendada nii teoreetilisi teadmisi kui ka praktilisi oskusi, tegelemaks infosüsteemide turvalisuse, digitaalsete tõendusmaterjalide ning arvuti turvaintsidentidega. Võimalik on läheneda nii tehnoloogilise, teoreetilise kui ka organisatoorse nurga alt.

Küberkaitse magistriprogrammi sisseastumisprotsessi käigus tuleb Tallinna Tehnikaülikoolile esitada oma Curriculum Vitae ja motivatsioonikiri, sooritada simulatsiooniülesandeid sisaldav veebipõhine test ning läbida vestlus [21]. Magistriõppes on lävendipõhine vastuvõtt, mis tähendab, et vastu võetakse kõik kandidaadid, kes ületavad eelnevalt ülikooli poolt seatud punktisumma, ning õppekoht küberkaitse erialal on tagatud, kui vastuvõtuprotsessis on saadud vähemalt seitse punkti kümnest [20].

## Sisseastumistesti keskkond

Tallinna Tehnikaülikooli küberkaitse magistriprogrammi tehniline test sooritatakse RangeForce [22] virtuaalses keskkonnas. Tegemist on pilvepõhise platvormiga, mille eesmärgiks on jäljendada tõsielulisi ründestsenaariume, võimaldades küberturbe spetsialistidel, arendajatel ja DevOps valdkonna töötajatel enda oskusi pidevalt proovile panna.

Pärast ülikoolile sisseastumisavalduse esitamist edastatakse kandidaadile unikaalne promokood, millega Rangeforce keskkonnale ligi pääseb. Sisseastumistest koosneb neljast laborist, millest on soovituslik sooritada vähemalt üks. Sisseastumistestil käsiteldavad teemad hõlmavad muuhulgas näiteks Linux CLI, Apache, HTTPS ja SQLi valdkondi.

Kuna test on veebipõhine ja selle sooritamiseks ei pea Tallinna Tehnikaülikooli füüsiliselt kohale tulema, kaasneb kandideerimisprotsessil matkimis- ehk kehastusrünnaku (*impersonation*) oht. Nimelt võib avalduse esitanud kandidaat otsustada, et konsulteerib testi tegemise ajal mõne endast targema isikuga või laseb kogunisti terve testi sooritada variisikul ehk kellelgi teisel kui endal. Viimast juhtu on antud töös nimetatud ka kehastus- ehk matkimisrünnakuks. Kuna test sooritatakse enne vestlusvooru, on kahtluste esinemise korral võimalik testi kohta täpsustavaid küsimusi esitada vestlusel.

# Senised saavutused

Alljärgnevalt on välja toodud mõningad lahendused veebipõhise õppe ja eksamite rikkumatuse tagamiseks nii akadeemilises kui kommertssektoris.

## Akadeemilised uuringud/lahendused/ideed/ettepanekud/katsetused

Fenu et al kasutab veebipõhise õppe puhul kehastusrünnaku vältimiseks multibiomeetrilist pidevtuvastussüsteemi (vt peatükk 4.2), mille eesmärk on vältida ülesande- ja seadmespetsiifilisust, see tähendab, et tuvastus töötab erinevat tüüpi ülesannetega (tekstivastus, valikvastus, suuline vastus jm) ja nii süle- ja lauaarvutite kui ka tahvlite ja mobiiltelefonide korral [23]. Nende lahendus kontrollib nägu, häält, puudet, hiirt ja klahvivajutusi, tuvastamaks kasutajat kogu kursuse vältel.

Multimodaalsusele keskendub ka Traoré et al, kes soovitab pidevtuvastuseks kombineerida näotuvastust, hiire kasutusviisi ja trükkimise dünaamikat, põhinedes kasutajal juba olemas oleval riistvaral (veebikaamera, hiir, klaviatuur) [16]. Infot antud biomeetriliste näitajate kohta kogutakse eksami jooksul passiivselt ehk kasutajat häirimata ning lubamatu käitumise (matkimisrünnak, eksaminandi lahkumine kaamera vaateväljast, mitu isikut eksamit lahendamas) esinemisel teavitati eksami järelevalve teostajat. Nende pakutud raamistik leidis kasutust ExamShield platvormi arenduses.

Clarke et al kirjeldab enda kaitsesüsteemi ideed kui õppesüsteemi kohal asuvat vihmavarju, mis pakub võimalust kasutajat tuvastada ja jälgida ilma õppesüsteemi tegevusse sekkumiseta [24]. Nende e-Invigilator’i puhul puuduks vajadus alla laadida lisatarkvara, kuna tegemist on brauseripõhise lahendusega. Oma töös implementeerisid nad vaid näotuvastuse osa.

Amigud et al keskendub sisuloome alusel kasutaja tuvastamisele [25]. Nimelt leitakse, et ühe ja sama tekstilise ülesande lahendamiseks kasutatav kirjutamisstiil, -mustrid ja sõnavara erinevad inimeste lõikes ning nende alusel on võimalik isikut tuvastada. Amigud et al andmeanalüüsil põhinev lahendus tuvastas teksti autori 93-protsendilise täpsusega. Võrdluseks, et kursuste juhendajad suutsid tudengite kirjastiili alusel pettust avastada vaid 12% juhtudest.

Mothukuri et al on oluliseks pidanud lukustusbrauseri olemasolu (vt peatükk 4.5), mis takistab ligipääsu keelatud programmidele ja funktsioonidele, ja näo- ning hääletuvastuse rakendamist, tuvastamaks ruumis esinevaid kõrvalisi isikuid [26].

Carlisle et Baird pakuvad välja spetsiaalse CD-lt buutiva lukustussüsteemi, milles on asendatud tavapärane failide avamise ja sulgemise dialoogaken [27]. Failid salvestatakse krüpteeritult kasutaja arvuti kõvakettale, millele testi sooritamise ajal ligi ei pääse, ja krüpteerimata kujul RAM-kettale, kust kasutaja neid avada saab. Blokeeritud on võrguühendus, USB-pesad, paremklikk ja kuigi lukustussüsteemi saab jooksutada virtuaalmasinas, märgistatakse sellisel juhul salvestatud failid ning neid ei krüpteerita.

Mõningad teaduslikud uuringud on näidetena eraldi välja toodud ka vastavate kaitsemeetmete juures (vt peatükk 4).

## Kommertslahendused

Eksisteerivad laiatarbelised eksami järelevalve lahendused jagunevad üldpildis neljaks.

Kõige traditsioonilisem neist on eksami sooritamine kontrollitud keskkonnas, nagu eksamikeskus või eraldatud ruum ülikoolis. Testi tegemise ajal jälgivad kandidaate vaatlejad, kelle ülesandeks on tuvastada ebaausat käitumist, nagu spikerdamine, kaaslasega konsulteerimine või keelatud abivahendite kasutamine. Kuna vaatlejateks on enamasti sama asutuse töötajad, võib kindel olla, et nad on kursis spetsiifiliste reeglitega, mida asutus eksamite korral rakendab, nagu näiteks sobiv riietus või lubatud abivahendid [28]. Kahjuks aga ei suuda ülikoolid enamasti palgata piisaval hulgal vaatlejaid, et tuvastada kõik ebaausa käitumise katsed. Veebipõhiste kursuste korral muudaks kohustus füüsiliselt eksamikeskusesse tulla eksaminandide elu keerulisemaks ja MOOCide ehk vaba juurdepääsuga e-kursuste puhul oleks taoline nõue mõeldamatu.

Reaalajas võrgujärelevalve korral kontrollitakse kandidaati kogu testi lahendamise vältel. Vaatluse all on nii ekraanil toimuv kui ka eksami sooritaja ise näiteks ekraanijagamistarkvara, mikrofoni ja veebikaamera pildi vahendusel [29]. Järelevalvet teostab ideaalis isik, kes on läbinud vastava koolituse ja oskab tähele panna petmisele viitavaid märke. Kuigi taoline lahendus võimaldab eksamit sooritada asukohast sõltumatult, eeldab see siiski ühise aja kokku leppimist ja sobiva kvalifikatsiooniga vaatleja palkamist ning on sellest tulenevalt järgnevatega võrreldes majanduslikult kulukam ja raskesti vajadusele kohandatav, kuna üks vaatleja suudab korraga jälgida vaid nelja kuni kümmet õpilast [30].Ka siin ei pruugi vaatleja märgata kõiki rikkumisi, kuid kuna kandidaat ei tea, millisel ajahetkel just teda jälgitakse, võib väheneda soov petta [28]. Mõned firmad pakuvad eksami järelevalve teenust koos enda poolsete vaatlejatega, kuid erinevalt kohaliku akadeemilise personali kaasamisest protsessi ei saa firmade puhul kindel olla, et vaatlejad on usaldusväärsed ja kursis konkreetse asutuse eksamireeglistiku ja akadeemiliste tavadega. Reaalajas võrgujärelevalvet pakub näiteks Pearson VUE [31]. Valikvastustega testi puhul saab tulemuse teada kohe. Õendustudengite seas läbi viidud uuring paljastas, et testitegijad tunnevad end ebamugavalt, kui neid veebikaamera vahendusel jälgitakse [32].

Salvestatava järelevalve puhul lindistatakse heli- ja videoseadme abil eksaminandi ennast ja tema arvutiekraanil olevat pilti, mida vaatleja hiljem mitmekordsel kiirendusel kontrollib, et analüüsida hetki, mil võis aset leida pettus [33]. Kuigi antud lahendus ei nõua, et eksami sooritamine ja järelevalve toimuksid samaaegselt, ning võimaldab sooritust vaadata tempokamalt kui reaalajas, on kontroll siiski jätkuvalt seotud inimfaktoriga, mille usaldusväärsuses ei saa kindel olla juhul, kui tegemist pole vastavalt kvalifitseeritud personaliga. Samuti tekib viivitus eksamitulemuste teada saamisel, kuna eelnevalt tuleb kindlaks teha, et tudeng ei ole reegleid rikkunud. Positiivse poole pealt säilib eksamist digitaalne tõend, mis hõlbustab hilisemate apellatsioonide lahendamist. Antud valdkonnas on pikalt tegutsenud Software Secure firma [34].

Hetkel on kõige tehnilisem lahendus automaatne järelevalve, mis sarnaselt eelnevatele eeldab ekraani ja kandidaadi lindistamist, kuid lisaks sellele analüüsib süsteem jooksvalt heli ja videopildi andmevoogu, tuvastamaks kahtlustäratavat ja ebasobivat käitumist [33]. Erinevate algoritmide abil kontrollitakse ruumi valgustust, kaadris asuvaid kahtlaseid objekte, eksamineeritava keskendumist ekraanile, taustaheli ja -pilti. Näotuvastus kindlustab, et testi sooritab üks ja sama isik. Ohukohad märgistatakse ning kuigi teoreetiliselt peaks kogu järelevalvega hakkama saama automaatsüsteem, on neid soovi korral võimalik hiljem ise üle kontrollida. Inimesest vaatleja puudumine tähendab, et ei eksisteeri piirangut eksami sooritamise ajale ja kohale, ning kogu süsteem muutub paremini vajadusele kohandatavaks, võimaldades kandidaatidele seada lisatingimusi näiteks piiratud operatsioonide, kindla IP-aadresside vahemiku või teiste rakenduste avamise takistamise näol. Kõiki kandidaate koheldakse võrdselt, sest vaatlejaks on algoritm, mitte inimene [28]. Soovi korral on eksaminande ka testi sooritamise ajal võimalik teavitada potentsiaalsest rikkumisest, tuletamaks meelde reeglistikku ja võimaldamaks selle alusel käitumist parandada. Kahjuks ei ole olemasolevad automaatsed järelevalvesüsteemid veel piisavalt head, et osutuda majanduslikult kasumlikuks. Mõned olukorrad märgitakse valepositiivselt ning mõned tagasihoidlikumad spikerdamiskatsed jäävad arvutil märkamata, mis tähendab, et lõpliku kontrolli peab jätkuvalt teostama inimene. Ühe Software Secure kliendi puhul märgiti 100 000-st toimunud eksamist potentsiaalseid pettuseid sisaldavaks 2425, millest reaalne rikkumine toimus 613 eksamil [30]. See tähendab, et algoritm tuvastas rikkumisi vääralt 75% juhtudest. Samuti ei saa automaatset eksamijärelevalvet kasutada, kui lubatud on abimaterjalid, sest süsteem ei tee vahet õpikul ja muudel märkmetel. Täisautomaatse järelevalvega testimist pakub firma Talview [35].

### Talview - Remote Proctor/Proview

Talview on Indiast alguse saanud firma, mis on keskendunud nii tööle kui ülikooli kandideerimise protsessi sujuvamaks ja veebipõhisemaks muutmisele [36].

Proview järelevalvesüsteem võimaldab vältida spikerdamist ja kontrollitavaks kehastamist ja lubab kokku hoida testide administreerimiskuludelt [35]. Salvestatakse eksamitegija ekraanil toimuvat ning ümbruses olevat heli ja videot. Süsteem kindlustab, et kandidaat keskendub testi tegemise ajal ekraanile, ruumis on piisavalt valge, taustal pole kahtlasi esemeid ega heli. Sisse logivat kasutajat autenditakse isikut tõendava dokumendi alusel näotuvastusega ning sama funktsionaalsust kasutatakse, kontrollimaks, et kandidaat ei vahetu testi tegemise ajal ehk eksamit teeb kogu protsessi vältel üks ja sama isik. Algoritm tuvastab võimalikud eksamikorra rikkumised ja teavitab nendest jooksvalt testi tegijat, võimaldades tollel parandada oma niinimetatud terviklikkuse või aususe skoori (*integrity score*), mis on alustades 100 punkti, aga kahaneb iga rikkumisega [37]. Testi sooritamise jooksul kogutud info edastatakse krüpteeritult põhjaliku logina vaatlejale, Proview firma ise videoid ei näe. Iga tudengi kohta, kelle aususe skoor on alla eelnevalt administraatori poolt määratud piiri, esitatakse foto autentimisprotsessist, taustamüra ja ekraanil toimuva kokkuvõte, suvalisel hetkel tehtud pildid ekraanist ja kandidaadi näost ning video eksamiprotsessist, mida on vaatlejal hiljem võimalik 60-kordse kiirusega järele vaadata, et teha kindlaks, kas protseduurireegleid ka tegelikult eirati. Piisava punktisumma korral antud andmeid vaatlejale ei edastata, mis tähendab ühtlasi privaatsemat kogemust iga ausa testitegija jaoks. Korraga on võimalik ühel ekraanil jälgida kuni 64 kandidaati [38].

Kuna Proview on oma olemuselt Javascripti skript, on seda võimalik integreerida ükskõik millise testimissüsteemi või veebilehega, toetades seega ka testi sooritamist mobiilseadmetes. Kandidaatidel puudub vajadus eraldiseisvate rakenduste või veebipluginate allalaadimise järele ning eksami sooritamise aeg ja koht ei ole välise vaatleja poolt piiratud, kuigi soovi korral on testi administraatoril võimalik kandidaate reaalajas jälgida. Proview ei piirdu vaid eksamite ajal tudengite isiku kontrollimisega, vaid võimaldab kogu kursuse vältel kindlaks teha, et ülesandeid lahendab üks ja sama tudeng. Lisaks eksamite vaatlusele ja õppetööle saab seda kasutada ka veebipõhiste intervjuude või muu suhtluse kontrollimiseks.

Miinimumnõuded Proview kasutamiseks hõlmavad vähemalt 640x480 eraldusvõimega veebikaamera, mikrofoni, Chrome või Firefox veebilehitseja olemasolu [37]. Proview toetab operatsioonisüsteeme alates Windows Vistast ja Mac OS X 10.5. Edukaks kasutamiseks peab interneti allalaadimiskiirus olema vähemalt 768 kbit/s ja üleslaadimiskiirus 384 kbit/s ning läbilaskevõime minimaalselt 256 kbit/s, kuigi soovituslik on 512 kbit/s. Vajalik on 1024 MB vaba mälu (RAM). Nõuetele vastavust kontrollitakse eraldi riistvaratesti abil, mille kestus on vähem kui 90 sekundit.

Lisaks täielikult automatiseeritud testimisjärelevalvele pakub firma ka Talview Proctor Engine’il põhinevat täielikku eksamikeskkonda, võimaldades muuseas kontrollida lugemist, kuulamist, kirjutamist, grammatikat, programmeerimisoskust [39]. Talview lahendusi kasutab näiteks Cambridge English Language Assessment [40].

### Software Secure - Remote Proctor PRO

Software Secure alustas järelevalve pakkumist tark- ja riistvara ühislahendusest, võimaldamaks kontrollida kaugõppe eksamitel toimuvat. Lahenduse põhiobjektiks oli seadeldis Remote Proctor PRO, mis koosnes 360-kraadi kaamerast, mikrofonist ja sõrmejäljelugejast [41].

Esiteks sisenes eksaminand oma õppekeskkonda (näiteks Moodle) [42]. Seejärel tuvastati arvutiga ühendatud Remote Proctor PRO seadme abil kandidaadi isik, võrreldes hetkebiomeetriat kursusega liitumisel registreeritud sõrmejälje ja näopildiga. Kui autentimine ebaõnnestus või seadeldis polnud arvutiga korrektselt ühendatud, keelati eksamil osalemine. Kui kasutaja oli edukalt tuvastatud, käivitus testimisprogramm Securexam, mis võimaldas eksami sooritamise ajal kasutada ainult õppekeskkonda ja blokeeris kogu ülejäänud funktsionaalsuse, kaasa arvatud ligipääsu failidele, internetile ja muudele rakendustele.

Testi tegemise ajal lindistas Remote Proctor PRO seadeldis muutusi ruumis aset leidvas liikumises ja helis. Kogutud andmed saadeti internetiühenduse kaudu Software Secure serverisse, kust neid vaatasid hiljem veebiliidese vahendusel üle Software Secure palgatud tunnustatud spetsialistid, kelle ülesandeks oli tuvastada eksamikorra rikkumisi, nagu kõrvaliste materjalide või abi kasutamine. Videosalvestis ja ülevaade eksamisooritusest koos potentsiaalsete pettushetkedega edastati asutusele, kes langetas lõpliku otsuse kandidaadi reeglite vastu rikkumise kohta.

Kui eksaminandi internetiühendus katkes eksami sooritamise ajal või polnud piisavalt kvaliteetne videofailide edastamiseks, üritas Remote Proctor PRO tarkvara faile edastada iga kord, kui eksamitegija arvuti uuesti käivitati. Remote Proctor PRO 360-kraadi kaamera ja sõrmejäljelugejaga lisaseadet Software Secure lehel enam ei müüda [43], aga seda on võimalik osta näiteks eBayst või Amazonist [44]. Aastal 2010 oli õpilastele seadme maksumus 200 $ ja järelevalvetarkvara hind 30 $ semestris [45], mistõttu oli tegemist üsna kalli lahendusega. Küll aga saab seadet kasutada korduvalt, st mitme isiku autentimiseks, mistõttu võis pärast kasutust selle edasi müüa või seda ülikoolidelt rentida.

### PSI - Remote Proctor Now

Alates aastast 2017. kuuluvad Software Secure firma ja nende lahendused PSI Services LLC omandisse, laiendades seni tööjõu kvalifikatsiooni kontrollimisele keskendunud firma pädevusala ka akadeemilisele poolele [46]. Hetkel kasutusel olev järelevalvelahendus Remote Proctor Now (RPNow) ei kasuta kandidaatide jälgimiseks enam välist seadeldist, vaid kandidaadi internetiühendusega arvutit, veebikaamerat ja mikrofoni, ning on täielikult veebi- ja pilvepõhine. Platvorm on LTI toe olemasolul seotav ükskõik millise õppekeskkonnaga (näiteks Moodle [47]), mis tähendab, et eksamiparoolid, -ajad, tulemused ja muu õppeinfo on automaatselt sünkroniseeritud, vähendades vigade tekke ohtu andmete ümber kandmisel. Tänu sellele võimaldab RPNow hõlpsalt õppekeskkonnas loodud arvutipõhistele eksamitele järelevalvet lisada ja tulemusi hallata.

Õppejõud või eksameid administreeriv isik saab endale harjumuspärases õppekeskkonnas luua eksami ning seejärel RPNow integreeritud keskkonnas seadistada, kui kaua eksam kestab, kas antud eksamile on vaja järelevalvet, millised on eksamil lubatud rakendused, veebilehed ja lisamaterjalid [48], [34], [49].

Eksaminand peab esmalt alla laadima Flash-i kasutava RPNow Secure Browser veebilehitseja, mis kontrollib käivitudes veebikaamera, mikrofoni ja piisavalt kiire internetiühenduse (üleslaadimiskiirusega 125 kbit/s) olemasolu ja et arvutiga ei oleks ühendatud välist ekraani. Sobiva eksami valimisele järgneb kandidaadi autentimine, mille käigus peab tegema foto nii kandidaadist endast kui ka tema isikut tõendavast dokumendist (pass, ID-kaart) ning lindistama video ümbritsevast ruumist, veendumaks, et läheduses pole keelatud materjale või kõrvalisi isikuid. Kui autentimine on edukas, suunatakse eksaminand läbi RPNow veebilehitseja asutuse õppekeskkonda (Moodle), kus küsitakse eksami salasõna, mille RPNow sisestab krüpteeritult tudengi nägemata, takistamaks testi sooritamist otse õppekeskkonnas väljaspool RPNow platvormi. Testi tegemise jooksul lindistatakse kandidaadi arvutiekraanil ja ruumis toimuvat heli ja videopilti. Kui kandidaat üritab käivitada rakendust, mille testi administraator on eelnevalt keelanud, takistab RPNow programmi avamist ja kuvab hoiatusakna.

Eksamilindistust kontrollivad pärast testi sooritamise lõppu PSI poolt kvalifitseeritud vaatlejad, kes märgistavad lindistuses esinevad eksimused eksami haldaja (õppejõu, administraatori) poolt määratud eksamikorra vastu, nagu näiteks lubamata materjalide kasutamine, keelatud veebilehtede külastamine või eksaminandi isiku vahetumine. Kui vähemalt kaks vaatlejat on sooritusele hinnangu andnud, kuvatakse eksami haldajale õppekeskkonna PSNow-ga integreeritud lehel soorituste analüüs koos täieliku eksamivideoga, märgistatud rikkumisolukordade ja autentimisinfoga iga tudengi kohta individuaalselt.

PSI lahendusi kasutavad muuhulgas edX MicroMasters, Ivy Tech Community College, Clemson University, Purdue University [50].

### Pearson VUE

Lisaks ametlikes eksamikeskuses testimisele pakub Pearson VUE ka veebipõhist testimist, ilma et peaks kartma eksamireeglite rikkumist. Pearson VUE lahenduse puhul kasutatakse reaalajas võrgujärelevalvet [51]. Eksami sooritamiseks tuleb eelnevalt registreeruda ja kokku lepitud ajal testi lahendamist alustada. Eksaminande jälgivad veebikaamera ja Pearson VUE Secure Browser veebilehitseja vahendusel Pearson VUE poolt sertifitseeritud vaatlejad, kelle ülesandeks on tuvastada protseduurireeglite rikkumisi [31].

Enne eksami algust luuakse ühendus tervitajaga (*greeter*), kelle ülesandeks on isikut tõendava dokumendi alusel tuvastada kandidaat, korrata üle reeglistik, teha kindlaks veebikaamera ja mikrofoni korrektne töötamine, teostada videokaamera vahendusel põhjalik kontroll testimiskeskkonna nõuetele vastavuse kohta: et ruumis ei viibiks kõrvalisi isikuid, et keskkond oleks piisavalt valgustatud, et keelatud abimaterjale, kaasa arvatud spikrid, lisamonitorid, -arvutid, maalid või postrid seintel, poleks nähtaval või riiete ja juuste vahele peidetud [52]. Kui kandidaat on autenditud ja protokolli vastu eksimisi ei tuvastatud, luuakse ühendus vaatlejaga (*proctor*), kellega saab tehniliste probleemide ilmnemisel vestlusakna kaudu ühendust võtta. Eksam võidakse koheselt kuulutada mittesooritatuks, kui kandidaat lahkub toast, väljub kaadrist või kui ruumi siseneb kõrvalisi isikuid.

Pearson VUE kasutamiseks peab olemas olema veebilehitseja (Internet Explorer 9 või uuem, Microsoft Edge, Chrome, Firefox, Safari), väline või sisseehitatud mikrofon ja veebikaamera eraldusvõimega vähemalt 640x480 [52]. Eksami ajal on lubatud kõrvaklappide kasutamine. Toetatud on operatsioonisüsteemid alates Windows 7 ja Mac OS X 10.8. Lairiba internetiühenduse alla- ja üleslaadimiskiirus peab olema 512 kbit/s, Pearson VUE ise soovitab kaabliühenduse kasutamist. Arvuti ja lisatarvikute tehnilistele nõuetele vastavust on võimalik kontrollida ükskõik millal enne eksami alustamist.

Pearson VUE võimaldab soovi korral eksamit läbi viia ka ilma järelevalveta, võimaldades kandidaadil testi sooritada ajaliselt kellestki teisest sõltumata [51]. Pearson VUE reaalajas vaatlemise lahenduse abil testib kandidaate näiteks Microsoft [52].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Ekraanipildi jälgimine | Lisaseade | Integreeritav olemasoleva testkeskkonnaga | Vaatleja olemasolu vajalik |
| Talview Remote Proctor | JAH | EI | JAH | EI |
| Remote Proctor PRO | läbi lisaseadme | JAH | JAH | JAH |
| RPNow | JAH | EI | JAH | JAH |
| Pearson VUE | JAH | EI | EI | JAH |

# Kaitsemeetmed

Järgnevalt on esile toodud mõningad kaitsemeetmed, vähendamaks identiteedi jagamise ohtu ehk seda, et kandidaat laseb testi enda isiku alt sooritada kellelgi teisel, ja lähtudes tingimusest, et testimiskeskkonnaks on RangeForce, kus abimaterjalide kasutamine on lubatud.

## Kontrollitud ruum

Kõige kindlam viis, veendumaks, et kandidaat teeb eksamit ise ja protseduurireeglitele vastavalt, on nõuda testi sooritamist kontrollitud järelevalvega ruumis, nagu näiteks eksamikeskus, milles kasutatavaid lisaseadmeid, nagu näiteks arvutid, on eelnevalt võimalik seadistada täpselt nii, nagu korraldaja heaks kiidab. Kontrollitud ruumi puhul saab veenduda, et seintel või laudadel pole keelatud lisamaterjale nagu valemid või spikrid, valgustus on sobiv, eksaminandid istuvad üksteisest piisavalt kaugel ja saavad segamatult töötada.

Kontrollitud keskkonnas on enamasti ka vähemalt üks vaatleja. Riigieksamite puhul on selleks näiteks eksamikomisjon ja Sihtasutus Innove poolt sertifitseeritud välisvaatleja [53], ülikoolide puhul enamasti õppejõud ja/või nende abilised, kelle ülesandeks on jälgida, et ei eksitaks akadeemiliste tavade vastu, näiteks keelatud abimaterjale kasutades või kaastudengiga konsulteerides. Statsionaarõppe puhul tunnevad õpetajad ja õppejõud enamasti oma õpilasi nägupidi, mis takistab kellelgi teisel kandidaadina esinemist. Küll aga ei ole see välistatud eraldiseisvate eksamikeskuste ja selliste kursuste puhul, kus õpe toimub e-keskkonnas, aga eksami tegemiseks peab füüsiliselt kohale tulema.

## Isiku pidev autentimine

Isiku tuvastamise ehk autentimise võib üldpildis jaotada kaheks. Üheks protsessiks on isiku identifitseerimine ehk esitatavate andmete võrdlemine iga andmebaasis oleva isiku andmetega, leidmaks esitatud andmetele vastavat isikut [54]. Antud juhul on tegemist üks-mitu (1:N) seosega, kus ühe komplekti esitatud andmete puhul käiakse läbi mitu isikut, kuni leitakse vaste.

Teine protsess on isiku verifitseerimine, mille käigus üritatakse aru saada, kas andmed esitav isik on see, keda ta väidab end olevat [55]. Sellisel juhul võrreldakse isiku esitatud parameetreid konkreetse andmebaasis oleva isiku andmetega ehk teostatakse üks-üks (1:1) võrdlus. Tulemuseks on tõeväärtus vastavalt sellele, kas esitatud parameetrid vastavad andmebaasis sama isiku kohta käivatele varasemalt teada olevatele parameetritele või mitte.

Eelnevast tulenevalt võib autentimist ehk kasutaja tuvastamist defineerida kui õigel ajahetkel õigete privileegidega õigele isikule õige ligipääsu võimaldamist [54].

Kui kontrollitud keskkonna puhul on raske ette kujutada, et eksaminandid poole eksami pealt vahetuvad, et kellelgi teisel enda eest test ära teha lasta, siis koduses keskkonnas on seda juba märksa keerulisem jälgida. Staatilised süsteemid, kus kasutaja isikut kontrollitakse ainult sisselogimisel, ei ole veebitestide korral piisavalt turvalised ka juhul, kui kasutajat ei kontrollita mitte ainult kasutajanime ja parooli kombinatsiooni, vaid ka biomeetriliste näitajate, nagu sõrmejälg, näotuvastus või silmaiirise skaneerimine, alusel [56].

Kasutaja autenditakse sessiooni algul sisse logimise hetkel ning sessiooni vältel verifitseeritakse kasutajat pidevalt või periooditi [57].

Üks potentsiaalne meetod kontrollimaks, et testi tegemise vältel kandidaat ei vahetu, on testitegija isiku pidev tuvastamine (ka pidevtuvastus, pidevautentimine, *continuous authentication*), mille võib jaotada kaheks - aktiivne ja passiivne autentimine [56]. Aktiivse autentimise puhul võidakse kasutajalt teatud ajaperioodi tagant või mõne tegevuse järel nõuda spetsiifilise ülesande, mis kinnitaks tema isikut, täitmist, näiteks parooli sisestamine, silmaiirise skaneerimine, teatud fraasi trükkimine või lausumine. Passiivse pidevautentimise puhul kogutakse andmeid taustal ilma kasutaja töövoogu segamata, muutes süsteemi kasutajasõbralikumaks ja eelistatumaks kontekstis, kus kasutaja keskendumine on põhiline.

Nagu staatilist autentimist võib ka pidevtuvastust jaotada selle alusel, milliste faktorite järgi kasutajat tuvastatakse. Selleks võib olla midagi, mida kasutaja teab (salasõna, PIN-kood, turvaküsimuse vastus), mida kasutaja omab (ID-kaart, kiipkaart) või mis iseloomustab kasutajat ennast ehk biomeetria [58], [26], kusjuures viimane jaguneb veel omakorda füüsiliseks (nägu, sõrmejälg, silmaiiris) ja käitumuslikuks (trükkimisstiil, allkiri, kõnnak) biomeetriaks [59]. Kui füüsiline biomeetria on enamasti muutumatu ilma kehamodifikatsioonideta, siis käitumine võib aja jooksul muutuda kasvõi kogemuste kogunemise ja süsteemiga harjumise [60], väsimuse või asendi [57] tõttu. Turvalisem on loomulikult mitme teguri kombinatsiooni nõudmine ehk multimodaalne süsteem, ~~kuid võttes aluseks eelpool püstitatud tingimused, tasub RangeForce süsteemi baasil läbi viidava sisseastumistesti puhul keskenduda mitme kasutajat kirjeldava biomeetrilise või käitumusliku atribuudi kontrollimisele~~.

Kasutaja pidevtuvastus ei tööta, kui kogu protsessi vältel sooritab tegevusi (registreerumine, sisselogimine, testi lahendamine) variisik ja puudub võimalus kontrollida kandidaadi tegelikku isikut, näiteks valitsuse andmebaasis leiduvate dokumentide põhjal. Eestis pakub isiku identiteedi kinnitamiseks ideaalset võimalust ID-kaart, mis on riigipoolseks kinnituseks, et antud isiku nimi ja nägu kuuluvad kokku. Sellisel juhul on võimalik andmebaasist saadud nime ja näo kombinatsiooni võrrelda testitegija omaga ja veenduda, kas isik on see, keda ta väidab end olevat. Kahjuks või õnneks ei ole need andmed avalikult kätte saadavad, teostamaks visuaalset kontrolli dokumendifoto alusel, küll aga on võimalik sisselogimist ID-kaardi tarkvara kaudu kontrollida. Kui eksisteerib varasemalt kasutajaga toimunud interaktioon, võib kasutajat tuvastada varasemal suhtlusel põhinevate turvaküsimuste alusel.

Kuna kõige raskem on muuta kasutajat ennast iseloomustavaid faktoreid, on järgnevalt analüüsitud mõningaid biomeetrilisi ja käitumuslikke näitajaid, mille alusel võiks RangeForce süsteemi kasutajat testi tegemise ajal korduvalt tuvastada.

### Näotuvastus

Kõige esimesena võiks tulla pähe visuaalne vaatlus arvutit kasutava isiku tuvastamiseks. Näotuvastus põhineb näo eristatavate tunnusjoonte ruumigeomeetria analüüsimisel [54]. Selle meetodi puhul määratakse, millised on vaadeldavad tunnused, mida erinevate piltide puhul võrrelda, nagu näiteks ninaotsa, suu, silmade vahemaa, ega jälgita kasutaja muid muutuda võivaid tunnuseid, nagu näoilmed, -karvad või juuksed. Üheks oluliseks väljakutseks ja tuvastuse esimeseks sammuks on inimnäo eraldamine ümbritsevast keskkonnast/taustast ehk näoavastus.

**Saavutused.** Näotuvastusel kasutatakse näiteks närvivõrke ja masinõpet [61]. Aastal 2014 saavutas Facebook kombineeritud süva-närvivõrke kasutades DeepFace projekti raames kuulsuste fotosid sisaldaval andmestikul Labeled Faces in the Wild (LFW) tuvastustäpsuse 97.35% [7]. Edasiarendus DeepID3 küündis samal andmestikul lausa 99.53% täpsuseni [62], mis jääb siiski vaevu alla Google FaceNet’i 99.63 protsendist [63]. Võrdluseks, et inimene suudab nägusid tuvastada 97.5% täpsusega [7].

Näotuvastus eeldab kasutajalt veebikaamera olemasolu. Õnneks on nüüdisajal paljudel müügil olevatel sülearvutitel veebikaamera juba sisse ehitatud ja ka väliseid veebikaameraid on laialdaselt saadaval.

Näotuvastuse edukusel võivad rolli mängida mitmed kasutajast või keskkonnast tulenevad faktorid, nagu näiteks ruumi valgustus, peaasend või näos olevad lisaseadmed. Sobilik süsteem ei tohiks end lasta häirida prille kandvast kasutajast. Adekvaatne näotuvastus nõuab piisavat valgustust.

**Elavus.** Video ei ole tegelikult ei midagi muud, kui seeria järjestatud pilte, mistõttu saab näotuvastust edukalt kasutada ka videovoo puhul. Just video puhul on oluline kontrollida ka näo elavust, et vältida süsteemi petmist staatilise foto, eellindistatud video, 3D-mudeli [64] või -maski [65] esitamise abil. Staatilist fotot saab kontrollida, paludes kasutajal pead liigutada või silmi pilgutada. Video esitamise vältimiseks on võimalik kontrollida kasutaja fookuspunkti, kuvades suvalisse asukohta ekraanil mõne punkti, kuhu kasutaja vaatama peab, või paluda kasutajal suvalises järjekorras teatud suunas pead liigutada. Virtuaalreaalsustehnoloogia abil on võimalik fotode põhjal koostada ka juhitavat 3D-mudelit kasutaja näost, mida elavuskontrollide petmiseks kasutada [64]. Mobiilseadmete puhul saab elavuse kontrolliks lisaks kaamerale kasutada ka güroskoopi ja kiirendusmõõturit [66], kuid arvutite puhul tasub keskenduda fookuspunkti kontrollimisele, mida on lähemalt vaadeldud antud töö peatükis 4.3. Ekstreemsemaks võimaluseks oleks ka kasutaja emotsiooni ja reaktsiooni jälgimine, kuvades näiteks keset töövoogu ekraanile mõne ehmatava pildi või video. Too lahendus loomulikult häiriks kasutaja keskendumist ega ole seetõttu eelistatud. Xu et al on välja pakkunud mitmeid teisigi potentsiaalseid kaitsemeetodeid, nagu pulsist tekkiv perioodiline mikroerisus näotoonis või näo ootamatu valgustamine tava- või infrapunavalgusega, jälgides samal ajal, kas muutub ka esitatava kaadri valgustatus [64].

Kui näotuvastust kombineerida mõne muu ajutise näitaja analüüsimisega, on võimalik kasutajat tuvastada ka siis, kui ta istumisasend (poos) pole optimaalne või ta vaatab veebikaamerast kõrvale. Selleks saab kasutada näiteks riiete värvi jälgimist [67]. Sisse logides salvestatakse kasutaja näo all oleva piirkonna värv, mida hiljem biomeetriliste näitajate puudumisel uuesti kontrollitakse. Kui tuvastatakse kasutaja lahkumine arvutiekraani eest või muutus näojoontes ja/või riiete värvis, on alust arvata, et tegemist pole enam sama kasutajaga, misjärel süsteem lukustatakse. ~~Seetõttu ei ole antud lahendus sobilik inimesele, kes iga viie minuti tagant riideid vahetab :)~~

Traoré et al OpenCV-le toetuva algoritmi eesmärgiks oli veebikaamera kaudu ja näo järgi tuvastada rikkumisi veebipõhistel eksamitel [16]. Nende pidevautentimissüsteemi täpsus oli 100%, see tähendab, et süsteemil õnnestus alati tuvastada variisik. Näotuvastussüsteem lindistas eksamit, tundis ära ja verifitseeris kandidaati näo alusel ning teavitas vaatlejat, kui kandidaat lahkus eksami ajal arvuti eest, testi tegi variisik või testi lahendas mitu tudengit korraga. Probleeme põhjustas muutus testimiskeskkonnas, eriti valgustustingimustes. Näotuvastuse täpsus langes drastiliselt, kui muudeti laualambi asukohta või kustutati valgus.

Fayyoumi ja Zarradi välja pakutud lahendus võrdleb testile registreerumisel andmebaasi salvestatud fotot testi tegemise aegse veebikaamera videovooga [68]. Lisaks sellele tuvastatakse kahesekundiliste videolõikudega, kas kasutaja jälgib ekraani ja on keskendunud eksamiküsimustele vastamisele. Kui leitakse, et kasutaja tähelepanu on mujal ehk võib esineda olukord, kus eksaminand kasutab keelatud abimaterjale, hoiatatakse testitegijat testimiskeskkonna taustavärvi muutusega. Samamoodi teavitatakse kasutajat ka ebaõnnestunud pidevautentimisest. Kui teatud aja jooksul ei õnnestu kasutajat tuvastada, peatab süsteem töö ja palub asendit korrigeerida. Korduval ebaõnnestumisel eeldatakse, et toimub pettus. Võrgukoormuse vähendamiseks kasutab Fayyoumi ja Zarradi lahendus meetodit, kus 30 sekundi tagant tehtud kahe sekundi pikkusest videoklipist valitakse kliendipoolse rakenduse abil välja parima näoilme, eraldusvõime ja valgustustingimusega kaader, mis edastatakse analüüsimiseks serverile. ~~Peaasendi kui ühe kergema fookuspunkti määraja järgi on petmist tuvastatud varemgi [69].~~

**Baasfoto.** Näotuvastust kasutades on vaja algsel registreerumisel tehtud fotot, millega edaspidist videovoogu kõrvutada. Baasfoto puhul on oluline, et see pärineks võimalikult usaldusväärsest ja kontrollitavast allikast, sest vastasel juhul võib kandidaat võrdluseks esitada pildi variisikust, kes hiljem tema eest eksamit sooritab. Seega oleks sobiv näiteks kandidaadi riiklik isikut tõendav pildiga dokument, nagu ID-kaart või pass. Puhtalt visuaalsele vaatlusele toetudes ei saa muidugi lõplikult veenduda dokumendi autentsuses ning alati jääb alles kahtlus, et dokument on võltsitud, kuid seda probleemi ei saa kõrvaldada enne, kui dokumentide ehtsuse kinnitamiseks kasutatakse ühtset süsteemi, nagu see on Eesti ID-kaardi puhul. Üheks variandiks oleks eksaminandidelt nõuda Eesti e-residentsust, kuid e-residendiks hakkamine võtab aega, eeldab kohalikus riigis Eesti saatkonna või konsulaadi külastamist ning maksab 100 eurot [70], mistõttu ei ole see tõenäoliselt ainult sisseastumiseksami sooritamise eeltingimusena praktiline nõue.

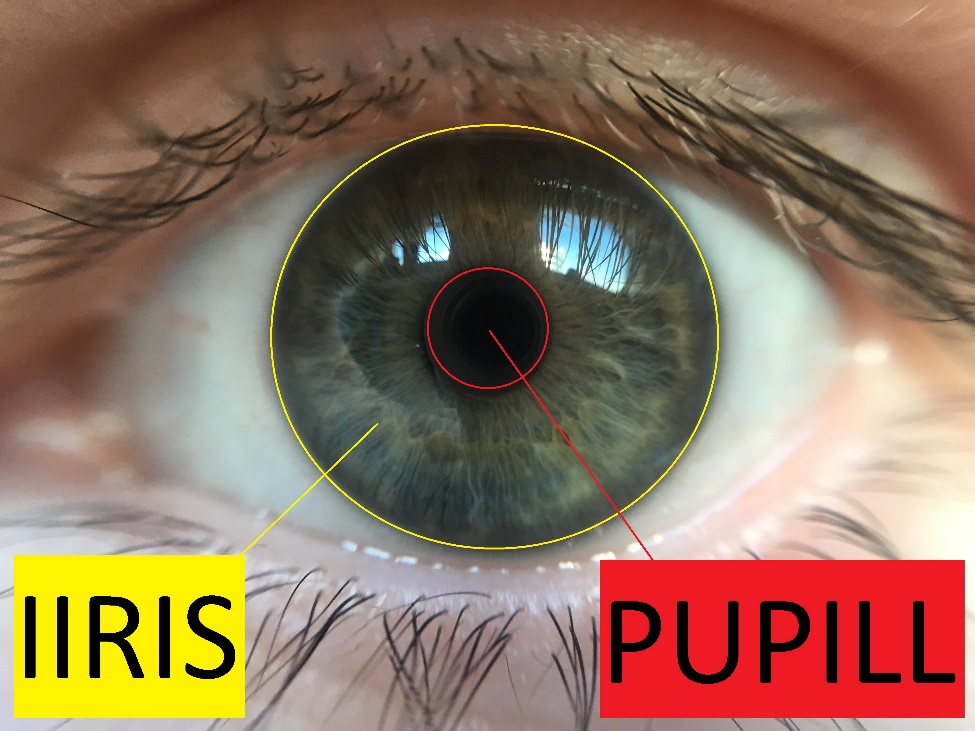
Video baasil pidevautentimise puhul võib probleemiks osutuda ka kogutud andmete saatmine üle võrgu serveripoolele, kus toimub nende analüüs. Edukaks edastamiseks on vaja piisavalt kiiret internetiühendust. Harjumuspäraste failiedastusprotokollide puhul kasutatakse kaadrite pidevaks edastamiseks liiga palju kasutaja arvuti ressursse (protsessor, mälu), mille tagajärjeks võib olla ühenduse katkestamine, edastuse aeglustamine või veebilehitseja töötamise lõpetamine. Ühendusega seotud probleeme oleks võimalik vähendada, kui algoritm töötaks lokaalses masinas. ~~Ühekordse veebipõhise eksamisessiooni puhul oleks see mõeldav, sest vaja on tuvastada, et kogu protsessi, mis ei kesta enamasti kauem kui mõni tund, vältel on arvuti ees üks ja sama isik~~. Andmehulka saab vähendada, kui analüüsida videovoogu perioodiliselt ehk võtta vaatluse alla ainult teatud ajahulga taga tehtud kaader [16]. Eksami puhul on see lubatud eeldusel, et analüüsitavate kaadrite vahele jääv ajaperiood on piisavalt lühike, et takistada inimeste vahetumist või tuvastada kõrvalise isiku esinemine ekraani ees.

Isegi, kui eeldada, et sisseastumiseksami kaitsesüsteem teeb edukalt vahet kandidaadi ja variisiku näol, ei ole ainult näotuvastuse rakendamine piisav kaitsemeede. Nimelt oleks sellisel juhul võimalik tekitada olukord, kus veebikaamera on kogu eksami vältel suunatud kandidaadi poole, aga testi lahendab sellest hoolimata keegi teine, kes kaamera vaatevälja ei ulatu. Ohuks on ka juhiste edastamine kandidaadile *bluetooth*-kõrvaklappide kaudu, mis on võimalik, kui ei kontrollita, et kandidaadi kõrvad oleksid katmata.

### Hääletuvastus

Üheks autentimismeetodiks on hääletuvastus. Pidevautentimiseks saaks seda kasutada suuliste eksamite puhul, kuid kuna küberkaitse eriala sisseastumiseksam RangeForce keskkonnas ei sisalda suulist osa, ei saa seda antud kontekstis kasutada kandidaadi isiku kontrollimiseks. Küll aga on võimalik tuvastada ümbritsevas ruumis olevat heli, et teha kindlaks, et keegi kandidaadile kõrvalt suulisi juhiseid ei edasta. Taustakõne keelamine töötab juhul, kui kandidaadil pole kombeks lahenduskäike iseendaga valjusti läbi arutada. Sisseastumiseksami puhul on vaikusenõue põhjendatud. Taustaheli analüüsist on räägitud käesoleva töö peatükis 4.6.

### Iirisetuvastus



Joonis . Silmaiiris ja pupill.

Iirisetuvastuseks nimetatakse biomeetrilist isikutuvastust, mis põhineb silma vikerkesta mustril [71]. Iiris on silma värviline osa pupilli vahetus ümbruses (Joonis 1), mille värvid võivad inimeseti korduda, kuid struktuur ja mustrid üldjuhul mitte, mistõttu pakub silmaiiris head võimalust kasutajate eristamiseks [72]. Vajalik on kvaliteetse kaamera olemasolu, et määrata küllaltki väikese iirise (diameetriga keskmiselt 11 mm) asukoht võimalikult täpselt. Enamasti kasutatakse selleks silma valgustamist infrapunase või lähi-infrapunase (*NIR - near infrared*) valgusega. Silmaiirise alusel kasutaja tuvastamine on kõige efektiivsem, kui iiris asub kaamerast maksimaalselt ühe meetri (1 m) kaugusel [17].

Kuna iirise korrektne tuvastamine nõuab eririistvaralist kaamerat ja kindlat vahemaad sellest, ei ole see taolisel kujul sobilik kasutaja pidevtuvastamiseks RangeForce sisseastumistesti raames ning käesolevas töös sellele laiemalt ei keskenduta, va katse fancy-pantsy Tobii-ga.

### Trükkimise dünaamika

Antud töös on sünonüümidena käsitletud termineid trükkimise dünaamika, klahvivajutuste dünaamika, trükkimisstiil.

Trükkimise dünaamika on hea meetod kasutaja tuvastamiseks, kuna ei nõua eririistvara, vaid tugineb klaviatuuri kui sisendseadme ja teatud klahvinuhi tarkvara olemasolule. Analüüsida saab nii klahvivajutuse kestust [73], erinevate klahvide vajutamise vahelist aega [74], trükkimisprotsessis esinevaid pause ja trükkimise tempot [75] kui ka seda, kas klahve vajutatakse eraldi või samaaegselt, mille erinevus tuleb esile suurtähti sisaldava fraasi puhul, kus võib kasutada nii Shift- kui CapsLock-klahvi (shift vs caps lock) [73].

Kasutajat saab (jooksvalt) tuvastada ka trükkimise visuaalsel või helilisel teel [76] või analüüsides klahvidele avaldatud survet [77] [78] - meetodid, mis nõuavad klaviatuurile ja kätele suunatud kaamerat käte asendi ja kuju jälgimiseks, mikrofoni klahvivajutustel tekkiva heli analüüsimiseks või vajutustugevuse kohta informatsiooni koguvat survetundlikku klaviatuuri. Võttes arvesse eeldust, et kasutajal on vaid üks veebikaamera, mis võib sülearvutite puhul olla integreeritud ja seega raskesti klaviatuurile suunatav, ja soovi kasutada ainult olemasolevat lihtsasti kätte saadavat riistvara, on surve, käte asendi ja trükkimise visuaalne analüüs antud töös kõrvale jäetud.

Kuna klahvivajutuste dünaamika puhul on tegemist käitumusliku biomeetriaga, on ründajal või variisikul seda äärmiselt raske imiteerida ka originaalkasutaja tegevuse vaatlemise tagajärjel [76]. Lisaks võib ajapikku kasutaja trükkimisstiilis esineda muutusi, mis on tingitud näiteks käte väsimisest pikaaegse kirjutamise tagajärel või oskuste kogunemisest [68] ja mis mõjutavad tuvastusprotsessi efektiivsust. Trükkimine võib ka sõltuda kasutatavast klaviatuurist ja selle harjumuspärasusest kasutajale [79].

Kasutaja korrektseks tuvastamiseks trükkimise baasil vajab süsteem eelnevat treenimist ja andmestikku [80]. Treenimisprotsess võib olla pikk ja keeruline [75], aga mida paremini koostatud algoritm, seda kiiremini tuvastatakse kasutaja vahetumine.

Trükkimisstiili saab kontrollida staatiliselt, näiteks parooli sisestamisel sisse logimise ajal. Eeldusel, et see protsess on varem korduvalt toimunud, on võimalik lisaks parooli korrektsusele käesoleva sisestuse trükkimisdünaamika andmeid võrrelda varasematega, et teha kindlaks, kas parooli sisestas sama isik, mis varem. USAs on võimalik küsimusi genereerida ka avalike andmete põhjal (nt eelmine postiindeks) [29]. Selline lahendus takistab kõrvalistel isikutel kontole ligi pääseda ka juhul, kui kasutaja parool ise on teada. Küll aga ei takista see kõrvaliste isikute ligipääsu juba alanud seansi korral [81]. Lisaks staatilisele tuvastusele on võimalik klahvivajutuste põhjal kasutajat autentida perioodiliselt [75], analüüsides trükkimist teatud hulga tähemärkide sisestamise või pausi esinemise järgselt, ja pidevalt [74]. Pidevtuvastuse puhul on oluline, et vale kasutaja tuvastatakse nii kiiresti kui võimalik ehk võimalikult väheste klahvivajutuste järel [59] ja et õiget kasutajat ei eemaldataks süsteemist esimese kõrvalekalde peale, vaid alles siis, kui usalduskvoot on langenud alla teatud piiri [59]. Bours et al töös oli selleks näiteks keskmiselt 182 tähtmärki [59]. Trükkimisstiili jälgimine on passiivne autentimisviis, kuna seda saab teostada ilma kasutajalt eraldi keskendumist nõudmata, ja protsess ei sega üldjuhul kasutaja tööjärge [75].

Mondal ja Bours olid ühed esimestest, kes analüüsisid ka ühe käega trükkimise tagajärjel tekkinud andmestikku ning kinnitasid püstitatud hüpoteesi, et ühe käega trükkimise tuvastuse edukus erineb suuresti mõlema käega trükkimise omast [74]. Seetõttu peaks süsteem arvesse võtma ka hetki, kus kasutaja sisestab teksti ajutiselt ainult ühe käega, ning ei tohiks kasutajat koheselt süsteemist välja visata.

Klahvivajutuste dünaamika salvestamiseks on parem töölauarakendus kui kergemini kasutatav ja arendatav veebipõhine lahendus, sest viimane sõltub suuresti platvormi tingimustest (veebilehitseja, RAM, protsessi prioriteet) ja ei tuvasta sageli funktsionaalseid klahve, nagu Enter, Control, Shift [79]. Töölauarapõhine rakendus võimaldab lisainfot koguda ka kursori liikumise ja süsteemiprotsesside kohta [79], laiendades kasutaja tuvastust ka hiire kasutusviisi arvelt.

Kuna RangeForce testid eeldavad käskude trükkimist virtuaalmasina terminalis, sobib kasutaja klahvivajutuste dünaamika analüüsimine eksaminandi identiteedi kontrollimiseks. Soovides suurendada analüüsitava trükiteksti hulka, võib testi sooritamise ajaks keelata kopeerimise ja kleepimise operatsioonid [79], mis tähendab, et isegi, kui eksaminand leiab veebist sobiva käsu, peab ta selle käsitsi ümber kirjutama, suurendades analüüsitavate klahvivajutuste andmestikku, mis omakoda võimaldab kasutajat täpsemini tuvastada. Võrdlusandmestiku genereerimiseks ja kaitsesüsteemi treenimiseks võib süsteemi sisse logides paluda sisestada enamlevinuid terminalikäske, mis ka ülesannete lahendustes esinevad.

Klahvivajutuste kogumisel on oluline andmestiku privaatsuse tagamine, kuna kogutud andmed võivad sisaldada kasutajanimesid ja paroole või tundlikku infot kasutaja enda kohta [79]. Tundlikud andmed tuleks enne trükkimisinfo salvestamist sellest kindlasti eemaldada või loobuda andmestiku salvestamisest. Kuna RangeForce testi puhul on kirjutamisstiili analüüsimine oluline vaid sessiooni vältel, tuvastamaks kasutaja vahetumist, ega vaja loodetavasti hilisemat uurimist, puudub vajadus andmete salvestamiseks. Lisaks ei nõua RangeForce ülesanded kasutajalt oma personaalsete andmete sisestamist, mistõttu ei saa sisestatud teksti nimetada tundlikuid andmeid sisaldavaks.

Seega võiks sobilik stsenaarium olla analoogne Roth et al pakutuga [76], kus süsteem käivitub parooli sisestades ja salvestab sellest momendist alates 30 sekundi jooksul kasutaja klaviatuuri kasutust, mis muutub edaspidise võrdluse baasiks kogu sessiooni vältel. Kui kasutaja lahkub arvuti tagant pikemaks perioodiks, sessioon lõppeb ja biomeetriline võrdlusbaas kustutatakse. Mõistlik on analüüsida kahe või enama klahvivajutuse kombinatsioone, näiteks kuidas erineb ’chown’ ja ’touch’ käske sisestades klahvivajutuste ’c’ ja ’h’ kestus ja vajutuste vahel olev aeg, kuigi see võib eeldada nende korduvat trükkimist enrolment-faasis.

Küll aga ei piisa ainult trükkimisprotsessi jälgimisest, sest see lubaks konsulteerida mõne teise ruumis viibiva isikuga, sisestamaks terminali nende ette öeldud käske. Samuti ei ole variisiku tuvastamine ainult trükkimise baasil kohene ja võtab aega [76], kuna nõuab võrreldava andmestiku kogumist.

### Hiire kasutusviis

Teiseks laialdaselt levinud sisendseadmeks on arvutihiir ja puutepadi (*touch pad*). Hiire puhul saab jälgida näiteks kursori asukohta eksaanil, hiire liigutamise suunda, kiirust, kiirendust ja sujuvust, liikumisvahemaad pikslites ja pausi tegevuste vahel [82], nuppude vajutamist ning lahti laskmist ja rulliku (*mouse wheel*) kasutamist [81]. Klikkimisel saab eristada üksikvajutust, topelt-klikki ja lohistamist. Eririistvaralise puutepadja puhul on võimalik analüüsida ka vajutuse survetugevust.

Ka hiiredünaamika jälgimisel on vajalik õppeperiood, et tuvastada konkreetsele kasutajale iseloomulik hiirekasutus. Tegelikult on hiire abil kasutajat lihtsam tuvastada pidevautentimisel kui staatilisel autentimisel [83], kus kogutavaid andmeid on kordades vähem. Sharif et al [84] implementeerisid andmestiku kogumise klahvivajutuste analüüsimise ja värviakna abil, kus kasutaja kindlas järjekorras neljal värviruudul klikkima pidi. Sayed et al [83] on selle probleemi lahendamiseks välja pakkunud närvivõrkudel põhineva sisselogimissüsteemi, kus kasutaja tuvastatakse sisselogimise ajal joonistatava sümboli järgi. Nii võib hiirekasutust võrrelda ka allkirjaga, mis peaks igal kasutajal olema unikaalne. Taolist alternatiivi traditsioonilisele salasõnaga sisselogimisele pakub näiteks BioMetric Signature ID [85].

Käesoleva töö autoril on näiteks komme oma harjumuspärast hiirt seda kasutades aeg-ajalt hiirematilt korraks kergitada ja seejärel samasse kohta tagasi asetada, mis põhjustab kursori koha peal jõnksutamist ja võib seetõttu olla üheks kasutajale iseloomulikuks jooneks.

Rose et al leidis, et vertikaal- ja horisontaalsuunas liigutatakse hiirt tavaliselt sirgjooneliselt, samas kui diagonaalidel tekib pigem kaarjas joon, kusjuures kaardumise kraad ja suund on iga kasutaja puhul unikaalne, pakkudes seega võimalust isiku tuvastamiseks [60].

Feher et al on võimelised kasutajat tuvastama kõigest ühe hiiretoimingu järel (to check!! sounds fishy) [57], suurendades nii sissetungija avastamise kiirust. Nende testgrupp kasutas nii optilisi hiiri, puutepatju (*touch pad*) kui ka krihvleid (*stylus*).

Mondal et Bours’i jõudsid masinõppealgoritme kasutades pidevtuvastuse lahenduseni [82], mille eesmärgiks oli, et terve sessiooni vältel ei tuvastataks tõelist kasutajat väärana. Oma lahendust katsetasid nad andmestikul, mis oli genereeritud arvutit igapäevaselt ilma mingisuguste piiranguteta kasutavate inimeste käitumisest. Ka nende eesmärgiks oli tuvastada kasutaja kõigest ühe hiiretoiminguga, mistõttu ei saanud nad kasutada statistilisi tunnusjooni, vaid üht sündmust iseloomustavaid iseärasusi. Kasutati Bours’i välja mõeldud usaldusmudelit, mille kohaselt õige kasutaja puhul usaldustase tõuseb ja vale puhul langeb, kuni alla teatud piiri langemist süsteem lukustatakse.

Dünaamika jälgimisel võib takistusi osutada hiire tüüp. Mehaanilise hiire puhul, mis ei ole küll enam nii levinud, võib funktsionaalsust mõjutada liikuvate osade vahele takerduv lint, optilisel hiirel valgust peegeldav või läbipaistev aluspind. Mõne hiire puhul tekib raskusi kiirete liigutuste salvestamisega [57]. Sõltuvalt oma füüsilisest asukohast (kodu, kool, ühistransport) võib sülearvuti kasutaja sisendseadmena kasutada kas välist hiirt või arvutile sisse ehitatud lahendusi, nagu osutushoob (näpuhiir, pointing stick, TrackPoint) või puutepadi (touch pad), millest sõltuvalt kasutusviis erineb ja valmistab raskusi kasutaja profiili koostamisel. Küll aga võib eeldada, et sisseastumiseksami lahendamise ajal kasutaja oma sisendseadet liiga sageli ei muuda. Erandiks võivad olla vaid sülearvuti omanikud, kelle puhul esineb olukord, kus intensiivse trükkimisprotsessi ajal eelistatakse kiireks hiireliigutuseks pigem puutepatja või osutushooba kui sülearvuti kõrval asuvat arvutihiirt.

Hiiredünaamikat tasub pidevautentimise täpsuskindluse tõstmiseks kombineerida klahvivajutuste dünaamikaga (vt peatükk 3.2.4) või silmade fookuspunkti analüüsimisega (vt peatükk 3.3).

### Hiire kaasabil autentimine

Hiire abil autentimine ei pea tähendama vaid kasutaja hiireliigutuste jälgimist. Kuna arvutihiire sisse on võimalik integreerida mitmeid autentimistehnoloogilisi lisalahendusi, saab hiirt kasutades jälgida kasutaja käelt kogutavaid andmeid. Sim et al on kasutaja pidevtuvastamiseks välja pakkunud idee kasutada sõrmejäljelugejaga hiirt [86]. Koos näotuvastusega pakub see kaitset, kui kasutaja sirvib veebilehti või e-posti, kasutades kerimiseks hiirt, kuid kuna trükkimise ajal on käed klaviatuuril ja peaasend on tavakasutajal pigem suunatud alla, ei ole tol hetkel võimalik kasutajat edukalt tuvastada. Seetõttu ei ole ainult hiirel asuva sõrmejäljelugeja ja näotuvastuse abil kasutaja autentimine praktiline. Üheks võimaluseks oleks lisada trükkimisdünaamika analüüs.

Küll aga on tänapäeval sõrmejälge arvestatavalt lihtne võltsida ning USA valitsusorganisatsiooni National Institute of Standards and Technology sõnul ei ole kahelt protsendilt inimkonnalt kvaliteetset sõrmejälge üldse võimalik võtta [87].

Liu et al [88] on uurinud kasutaja pidevtuvastamist käekuju ja -joonte kaudu juhtseadmele paigutatud sensorite abil. Nemad keskendusid juhtkangidele (*operating rod*), nagu on lennukil, mootorrattal või ekskavaatoril, aga tegelikult saab sama tehnoloogia üle kanda ka arvutihiirtele.

Midagi analoogset on teinud Fujitsu oma PalmSecure [89] tehnoloogiat toetava hiirega [90]. Peopesas asuvate veenide järgi autentimist peetakse hetkel kõige turvalisemaks biomeetriliseks tuvastusmeetodiks, sest veenide asetus on igal inimesel unikaalne, ei muutu elu jooksul ning ei sõltu välisteguritest, nagu temperatuur või niiskus. Infrapunase valguse abil veenivere hapnikusisalduse jälgimine raskendab suuresti antud biomeetrilise näitaja võltsimist. Kahjuks on käesoleval hetkel Fujitsu PalmSecure tehnoloogia puutevaba, mis tähendab, et kuigi veenimustri lugeja on spetsiaalse arvutihiire sisse integreeritud, on kasutaja tuvastamiseks tarvilik peopesa hiirelt tõsta ja kätt seadme kohal hoida, mistõttu ei ole tegemist täielikult passiivse ja pideva autentimismeetodiga.

Eelpool mainitud lahendused eeldavad spetsiaalse riistvaraga hiire olemasolu, mida ei saa sisseastumiseksami sooritajalt nõuda, mistõttu ei ole need antud kontekstis rakendatavad.

### Kergbiomeetria

Kergbiomeetriaks (*soft biometrics*) nimetatakse inimkeha eristatavatel välistunnustel (sugu, vanus, kasv, kaal, rass, nahavärv, silmavärv, juustevärv, armid, sünnimärgid, tätoveeringud) põhinevat liigituslikku, kuid enamasti mitte individualiseerivat biomeetriat [91]. Kuigi need tunnused pole unikaalsed ja neid on võimalik muuta ning võltsida (meik, kontsad, mask, parukas), annavad nad siiski kasutajast mõningase ülevaate, mistõttu saab neid kasutada koos teiste autentimissüsteemidega [92]. Kergbiomeetrilisi tunnuseid ei hoita andmebaasis, vaid need salvestatakse käesoleva sessiooni võrdluse tarbeks sisselogimise hetkel [93].

RangeForce puhul tasuks kaaluda näiteks soo, rassi, naha- ja juustevärvi ning näopiirkonnas olevate armide, sünnimärkide ja tätoveeringude jälgimist, kuna nende kohta on võimalik infot koguda veebikaamera vahendusel ja need kergbiomeetria tunnused toetaksid isiku kontrollimist videopildi ja näotuvastuse baasil.

### Muu

Kasutajat saab pidevtuvastada ka näiteks ajutegevuse alusel, jälgides pea külge kinnitatud anduritega ajusignaale või muutusi hemoglobiinis (veres) näiteks spektroskoopia või elektroentsefalograafia (EEG) abil [8]. Ajutegevus sõltub keskkonnast, ajutisest ja füüsilisest seisundist, kuid võrreldes ajutegevust puhkehetkel ja ülesande lahendamise (trükkimise) ajal võib inimeste lõikes näha mõningaid erinevusi, mille alusel kasutajaid tuvastada, kusjuures paremini ilmnevad need just puhkehetkel. Mida rohkem sensoreid, seda parem tulemus. Ajuaktiivsust jälgides on võimalik kontrollida, kas sensoreid kandev kandidaat tegeleb parasjagu sisseastumiseksami lahendamise või millegi muuga.

Ka elektrokardiogrammiga (EKG) südametegevust mõõtes on võimalik kasutajat autentida [12]. Küll aga võib südametegevuse abil kasutaja tuvastamine olla ajamahukam protsess, sest kui näiteks näopildi puhul on analüüsimiseks võimalik saada 30 kaadrit sekundis, siis süda lööb keskmiselt 1-1.5 korda sekundis, mistõttu kulub süsteemi treenimiseks kauem aega. Probleemiks võib osutuda ka füsioloogiliste ja psühholoogiliste muutuste, nagu kehaline aktiivsus, toitumine, haigused, hingamine või elektroodide asetus, mõju EKG signaalidele, mida tuleb sobivat robustset autentimissüsteemi disainides arvesse võtta. Ühe potentsiaalse dünaamiliselt kogutud andmete põhjal usalduskvoote muutva lahenduse, mis töötab ka väheste müra sisaldavate andmete peal ja paremini kui varasemad lahendused (EER = 7.89%), on välja pakkunud Louis et al [12]. Südemetegevuse mõõtmist autorooli integreeritud elektroodidega on kasutatud ka autojuhtide fookuse ja väsimustaseme kontrollimiseks ning nende pidevaks isikutuvastuseks [94].

Iga inimkeha reageerib erinevalt, kui seda mõjutada madalpinge impulsiga, sest elektrijuhtivus ja signaali nõrgenemise intensiivsus sõltub luustruktuurist, lihaste tihedusest, rasvasisaldusest ja veresoonte asendist ning suurusest [55]. Seetõttu saab kasutajat tuvastada, kui suunata ühte peopessa madalpinge elektriimpulss ja ülekande tulemust teisest peopesast mõõta. Kui teiste autentimismeetodite (näotuvastus, sõrmejälg) korral on süsteemide petmine taasesituse meetodil lihtne, siis keha reaktsiooni elektrilisele impulsile on äärmiselt raske replikeerida, kuna taasesitamiseks on vaja täpselt sama juhtivusega riistvara, mistõttu on tegemist ühe turvalisema tuvastusmeetodiga. Elektrit juhtivast materjalist või elektrit juhtiva kihiga kaetud klaviatuuri (ja hiire) olemasolul saab trükkimise ajal sõrmeotstel edastatud ja mõõdetud elektriimpulsse kasutada kasutaja pidevtuvastamise eesmärgil.

Ka nutikellade ja aktiivsusmonitoride sensoritest kogutud info (sammude arv, südamerütm/pulss, kalorikulu) abil on võimalik kasutajat tuvastada [95], kuigi antud meetodi puhul on kasutaja edukaks tuvastamiseks vaja laialdast võrdlusandmestikku kasutaja tegevuse ja kehalise aktiivsuse kohta. Küll aga saaks aktiivsusmonitore kasutada, kontrollimaks kasutaja reaktsiooni erinevatele stiimulitele, näiteks südamerütmi löögisageduse suurenemine äkilise ehmatava foto või videoklipi kuvamisel ekraanile.

Kõik antud peatükis mainitud tuvastusmeetodid on kasutaja jaoks passiivsed, see tähendab, et kasutaja tööjärge ei segata, vaid autentimine toimub taustal. Küll aga nõuavad käsitletud tuvastusmeetodid eririistvara või lisaseadmete olemasolu, mida ei saa kandidaatidelt nõuda, mistõttu ei ole ükski käsitletud meetod TTÜ küberkaitse sisseastumiseksami jaoks sobilik.

## Silmade liikumise ja fookuspunkti jälgimine

Silmade liikumine kuulub käitumusliku biomeetria alla. Silmaliikumisdünaamika puhul jälgitakse pilgu liikumist ekraanil. Sageli on selle professionaalselt tegemiseks vaja eririistvara, nagu peatugi [96], infrapunafiltriga kaamera ja infrapunase valguse allikas, et suurendada pupilli avastamise ja jälgimise täpsust, aga mõne lihtsama lahenduse puhul piisab ka sisseehitatud veebikaamerast. Silmade liikumise analüüs on ideaalne multibiomeetriliste süsteemide jaoks, eraldiseisvalt mitte nii väga [96]. Silmade liikumine sõltub nii nende füüsilisest ehitusest kui ka neuroloogilistest faktoritest [97], mistõttu on masina abil silma tegevuse imiteerimine keeruline [96]. Silmade liikumise dünaamika jälgimist kasutatakse muuhulgas kasutajaliideste ja reklaamide analüüsimiseks, silmahaiguste diagnoosimiseks [98] või sisendseadme asemel nende erivajadustega inimeste puhul, kes ei saa arvutit tavapärasel moel hiire ja klaviatuuri abil kasutada [99].

Probleemiks on peaasendi muutumine jälgimisprotsessi ajal [100] [101]. Kasutaja silmade või pea külge kinnitatavad süsteemid töötavad paremini kui arvuti küljes oleva kaameraga süsteem, mis ei võta arvesse kasutaja pea liikumist ekraani suhtes ja töötab hästi vaid seni, kuni peaasend on sama, mis kalibreerimise ajal. Üheks võimalikuks lahenduseks oleks kaasata näotuvastust ning näoasendi ja silmade positsiooni abil näos pilgu liikumise jälgimist parendada. Analoogse lahenduse näotuvastuseks ja pilgu jälgimiseks treenitud närvivõrguga on välja pakkunud Bäck [102] ja Cheung et Peng [98]. Bäck võttis pea asendit arvesse silmaiirise, välisnurga ja ninasõõrmete abil. Antud tunnusjooned valiti, kuna neid on ülejäänud näost lihtne avastada ja need ei sõltu kasutaja emotsioonidest. Bäcki süsteem ei tööta küll sama hästi, kui tol hetkel turul olevad, aga pakub siiski alternatiivi infrapunast kasutavatele lahendustele. Cheung et Peng-i arvutile ja veebikaamerale suunatud meetodiga eraldati samuti näokujutisest silmaala, millest omakorda tuvastati iirise keskme ja silma sisenurga (silmatorkavam ja vähem tundlik näoilme muutumisele kui välisnurk) asukoht, mille alusel pilgu suunda arvutada. Erinevate valgustingimuste (päevavalgus, LED-, luminofoorlamp) ühtlustamiseks/kompenseerimiseks ja näopiirkonna eraldamise hõlbustamiseks kasutati heledustasemete reguleerimist histogrammide abil. Pea asendi kalkuleerimiseks jälgiti mitmeid punkte põskedel, kulmudel, silmadel, ninal ja suul. Cheung et Peng-i välja pakutud lahendus suudab pilku jälgida ilma eelneva treenimiseta. Vähese peaasendi muutuse (kuni 15 kraadi) ja staatilise näoilme korral saavutati ligikaudu 2.27 kraadine täpsus.

Silmade kaadrist väljumist ja peaasendi muutumise mõju erinevatele olemasolevatele pilgujälgimislahendustele on uurinud näiteks [101], kes tõestasid, et antud valdkonnas on veel arenguruumi. Infrapunalahendusi kasutades võib takistavaks faktoriks osutuda ka prillide kandmine, sest klaasid võivad peegeldada arvutiekraanilt tulevat valgust ja takistada seega silma tuvastamist. Tavavalgust kasutades pole prillide kasutamine niivõrd suureks takistuseks [98]. Kindlasti nõuavad pilgujälgimisrakendused eelnevat kalibreerimist, et kasutaja pilgu suunda korrektselt jälgida.

Silmade fookust autentimise eesmärgil kasutamiseks on uuritud näotuvastust ja pilku ühendava SAFE autentimissüsteemi raames [103], kus kasutaja peab registreerimisel valima salajaste ikoonide kogu, millest suvaliselt valituna ühte hilisema autentimisprotsessi käigus sarnaste peibutusikoonide seast tuvastama ja silmadega jälgima peab. SAFE lahendus kasutab seadme (arvuti, telefon) esikaamerat, kaht infrapunavalguse allikat ja üht infrapunafiltriga kaamerat, mille abil tuvastatakse kasutaja pupillide asend ja liikumine.

Sirur et Pendse on välja pakkunud hääle, silmade ja pilgutamise kombinatsiooniga arvuti kontrollimise lahenduse [104], kus kasutaja kannab spetsiaalset kiivrit, mille külge on kinnitatud kaks kaamerat, filtrid ja infrapunase valguse allikas. Kuna silmaiiris ja pupill neelavad infrapunast valgust erinevalt, on võimalik paika panna pupilli asukoht ja vaate suund. Kaameratest saadava info põhjal arvutatakse välja kasutaja silmade vaatenurk ekraani suhtes ja kasutajale omased iirist kirjeldavad atribuudid, mille alusel on võimalik isikut tuvastada. Sirur et Pendse lahendus erineb eelnevatest selle poolest, et võtab enam arvesse ka asiaatide silmade ehitust ja silmamuna osaliselt katvat silmalaugu.

Eririistvarata on pilgujälgimist uurinud Sewell ja Komogortsev [105], kes kasutasid oma töös sülearvuti sisseehitatud kaamerat, koolile või kontorile sarnanevaid valgustingimusi ja närvivõrku, mis treeniti pupilli liikumist jälgima.

Silmade liikumise dünaamika sõltub täidetavast ülesandest. Sotsiaalmeedia veebilehte uurides liiguvad silmad teistmoodi kui RangeForce süsteemis küberkaitse sisseastumiseksamit lahendades. Seetõttu on see hea meetod kindlustamaks, et kaamera ees olev isik tegeleb aktiivselt eksami lahendamisega, mitte ei lase variisikul eksamit enda eest sooritada, olles ise sotsiaalmeedias, kaamera näotuvastuse abil autentimise tingimuse täitmiseks enda poole suunatud.

Antud kaitsemeedet oleks võimalik üle kavaldada, kasutades eksami lahendamiseks kaht ekraani, kus mõlemal kuvatakse sama pilt RangeForce testist, kusjuures kaamera on suunatud tegeliku kandidaadi, mitte variisiku, poole. Nii vastab tegeliku kandidaadi silmade liikumine testimiskeskkonna kasutamisel eeldatavale. Et sellist situatsiooni välistada, tuleb arvesse võtta, et silmade liikumine on korrelatsioonis hiire liikumisega. Kuna enamasti fikseeritakse esmalt silmadega arvutiekraanil fookuspunkt, kuhu seejärel hiirega liigutakse, mitte vastupidi, siis võib eeldada, et ilma valjusti oma kavatsustest tegelikule kandidaadile teada andmata ei saa variisik hiirt soovitud kohta liigutada nii, et tegeliku kandidaadi silmad keskenduksid kursori asemel ekraaniobjektile, millel lõpuks peatutakse. Omavahelist suulist ja kirjalikku kommunikatsiooni saab takistada ruumi heli analüüsides, märkides ohukohtadena inimkõne kostumise või trükkimisheli esinemise ajal, kui RangeForce süsteemis tekstisisestust ei toimu.

## Välise lisaekraani keelamine

Mõned võimalikud ründestsenaariumid kasutavad ära võimalust duplitseerida pilti mitmel monitoril. Näiteks võib silmade liikumist ja näotuvastust kasutavat kaitsesüsteemi petta, kui arvutis sooritab eksamit variisik, kuid näotuvastust teostav ja silmade liikumist analüüsiv kaamera on suunatud tegeliku kandidaadi suunas, kes jälgib variisiku eksamisooritust lisaekraanilt. Nii liiguvad kandidaadi silmad RangeForce süsteemiga kooskõlas ning keerulisem on tuvastada, et tegelikult kandidaat vaid jälgib ekraanil toimuvat. Sellest tulenevalt on oluline tuvastada lisaekraani olemasolu ning paluda kasutajal see eemaldada. Näiteks Windowsi operatsioonisüsteemi puhul on selleks võimalik kasutada funktsiooni EnumDisplayMonitors [106] või EnumDisplayDevices [107] ja Linuxil tööriista xrandr [108].

## Väliste rakenduste keelamine

Selleks, et eksaminand ei saaks testi sooritamise ajal suhtlusprogrammide kaudu abilistega konsulteerida, tuleks keelata välised rakendused nii kasutaja arvutis kui ka RangeForce virtuaalmasinas. Üks võimalus selleks oleks kasutada olemasolevaid ekraanilukustusprogramme, mis takistavad rakenduste vahelist navigeerimist testi tegemise ajal. Alternatiivselt võib disainida spetsiaalselt RangeForce sisseastumiseksami tarbeks koostatud turvalise veebilehitseja, milles on võimalik avada vaid sisseastumiseksami keskkond ja mis teavitab ülikooli, kui veebilehitseja aken pole aktiivne ehk on alust arvata, et kasutajal on tol hetkel lahti mõni teine programm. Turvalisest veebilehitsejast väljumise takistamiseks võib keelata hiire paremkliki, funktsiooniklahvid või muud akende vahel liikumist võimaldavad klahvikombinatsioonid (Ctrl+Alt+Del, Alt+Tab). Turul on mitmeid analoogseid kommertslahendusi, näiteks Respondus [109] või Safe Exam Browser [110], kuid kaaluda võib ka spetsiaalset CD-lt käivituvat lukustussüsteemi [27]

Alternatiivne variant on tarkvaraliselt teiste programmide avamine lubada, kuid pidada arvestust aktiivsete akende üle ja kui neid tuvastatakse lubatud limiidist rohkem, kuvada hoiatus, mis palub aken sulgeda, ning salvestada kuvapilt kasutaja ekraanist hilisemaks ülevaatamiseks. Küsides infot aktiivsete akende kohta operatsioonisüsteemi API-lt, on avastustäpsus 100% [111].

Kuna RangeForce test toimub virtuaalmasinas, tuleb otsustada, milliseid rakendusi ja veebilehti ning millisel määral blokeerida lokaalses masinas ja milliseid virtuaalmasinas. Koostöös RangeForce keskkonna arendajatega oleks mõeldav süsteemisiseselt sisseastumiseksami tarbeks ainult teatud rakenduste ja veebilehtede lubamine. Eksaminandidel on lubatud kasutada otsingumootoreid (Google, Bing), kuid keelatud vahetada infot suhtlusprogrammide (Facebook, VK) vahendusel. Seega peaks vähemalt ühes skoobis olema lubatud veebilehitseja kasutamine, aga piirangutega, nii et keelatud leheküljed oleksid blokeeritud. Tõenäoliselt oleks kõige lihtsam keelata kõik rakendused lokaalses masinas ja lubada osaliselt virtuaalmasinas, kus kontrollimine ja tuvastus on lihtsam. RangeForce virtuaalmasinas oleva veebilehitseja saab juba eelnevalt seadistada nii, et eksami läbiviija poolt loetletud veebilehekülgedele ligipääs puudub. Lisaks vähendab kontrolli viimine RangeForce keskkonna poolele ohtu, et eksaminand saab kaitsetarkvara saboteerida, näiteks selle lähtekoodi modifitseerides.

Lukustusbrauserit saaks petta, kui lokaalses masinas jooksutada virtuaalmasinat, milles omakorda käivitada lukustusbrauser, milles avaneb RangeForce test. Nii oleksid rakendused blokeeritud vaid kasutaja lokaalses masinas jooksvas virtuaalmasinas, mitte lokaalses masinas endas, võimaldades lokaalses masinas blokeeringust hoolimata kõrvalisi programme kasutada. Et selline olukord välistada, on vaja tuvastada, kas lukustusbrauser töötab virtuaalkeskkonnas või mitte. Selleks võib näiteks kontrollida/uurida hüperviisori olemasolu CPUID-d järgi [112], registrivõtmeid, mälu, virtuaalmasina ja hosti vahelist suhtluskanalit, protsesse ja faile, MAC-aadressi, BIOS-i seerianumbrit [113], väljuvate IP-pakettide TCP-päiste kontroll-lippe, eluiga, ID-sid [114] ja ajatempleid [115]. RangeForce testi lahendamiseks mõeldud lukustusbrauser ei tohi käivituda virtuaalmasinas. Selle asemel tuleb kasutajat tekkinud olukorrast teavitada, paluda virtuaalmasinat mitte kasutada ning brauser sulgeda.

Sellised ennetusmeetmed välistaksid ekraanijagamis- ja suhtlusprogrammide kasutamise nii lokaalses kui ka virtuaalmasinas. Alternatiiviks väliste rakenduste keelamisele võiks olla ka pidev või perioodiline kuvapildi jälgimine, tuvastamaks keelatud rakendusi, kuid lukustusbrauseri kasutamisel muutub kuvapildi eraldi jälgimine tarbetuks, mistõttu ei ole seda kaitsemeedet antud töös lähemalt käsiteldud.

Kui testitegemise keskkond on isoleeritud, tuleb aga kaaluda varianti, et eksaminand kasutab info edastamiseks ja juhiste saamiseks lisaseadmeid, nagu ruumis viibiv kõrvaline isik, teine arvuti või nutitelefon, mistõttu on oluline jälgida ruumi heli ja videopilti.

## Ruumi helianalüüs

Kui arvutipõhine suhtlus erinevate ekraanijagamise ja suhtlusprogrammide abil on keelatud, tuleks kontrollida ka seda, et infoedastus ei toimuks suuliselt või muude lisaseadmetega. Selleks oleks praktiline kuulata ruumi taustaheli ning tuvastada sealt inimkõne. Kuna sisseastumiseksami puhul on võimalik nõuda täielikku vaikust, välistades ka kandidaadi valjuhäälse arutelu, viitab taustal esinev kõne kõrvaliste isikute viibimisele ruumis.

Kõnetuvastust võivad häirida muud ruumis esinevad helid, nagu tooli liikumine, klahvivajutuste heli, hingamine, köhimine. Selleks, et iga vähimgi heli kõnetuvastussüsteemi ei käivitaks, võib analüüsida heli valjudust, sagedust või kestust ja süsteemi eelnevalt positiivsete (kõne, sosistamine) ja negatiivsete (hingamine, köhimine, konditsioneer, linnaliiklus) näidistega treenida [111]. Et välistada taustaheli analüüsimise saboteerimist mikrofoni blokeerimise või muu analoogse meetodi näol, võib ebaregulaarse perioodi järel kõlaritest kostuda lasta signaalil. Kui mikrofon helisignaali kinni ei püüa, on kandidaat helianalüüsile vahele seganud.

Samuti võib taustaheli analüüsimine aimu anda teise arvuti abil toimuvast kommunikatsioonist. Kui sisseastumiseksami kaitsesüsteem analüüsib klahvivajutusi, saab trükkimisheli esinemisel, aga klahvivajutuste puudumisel järeldada, et ruumis on ka teine klaviatuuriga seade, mille kaudu on võimalik infot edastada ja seega eksamikorda rikkuda.

## Ruumi pildianalüüs

Selleks, et takistada väljaspool kaamera vaatevälja olevate abivahendite kasutamist või kõrvaliste isikute viibimist ruumis, tuleks kandidaadil enne eksami algust lindistada 360-kraadine video ruumist, kus eksamit sooritatakse, kasutades selleks veebikaamerat. Oleks hea, kui tolleks hetkeks oleks võimalik luua ühendus inimesest järelevaatajaga, kes veenduks keskkonna sobilikkuses ja vajadusel paluks sobimatud esemed eemaldada, kuid kui see pole võimalik, tuleb eksaminandile koostada selge ja arusaadav juhend korrektse eksamikeskkonna ning lubatud materjalide ja seadmete kohta ruumis ning ruumist 360-kraadise ülevaate andev videoklipp hiljem eksami läbiviijal manuaalselt üle vaadata.

Ruumi tuleks veebikaamera videopildi vahendusel analüüsida ka hiljem, eksami sooritamise ajal, veendumaks, et protsessi käigus ei lisandu ruumi inimesi. Selleks võib kasutada näotuvastust, jälgides lisaks esiplaanil oleva eksaminandi näole taustale tekkivaid näokujutisi, või liikumisanalüüsi, märgistades ohukohtadena kaadris toimuva lisaliikumise. Liikumise analüüs peaks olema võimalikult robustne ja pigem vähetundlik, kuna vastasel juhul võib see iga eksaminandi toolis tahapoole nõjatumise märgistada kui taustaliikumise. Üks võimalus oleks siinkohal eeldada, et eksaminandi keha asub vahetult tema näo all [67], [93] ning analüüsida liikumist piirkonnas, mis ei ole märgistatud kui pea või keha ning loetakse seetõttu taustaks. Antud juhul võib süsteemi vallandada kasutaja ringutamine.

Kõrgtasemelise süsteemi puhul võiks kaaluda erinevate esemete, näiteks telefon, lisaarvuti, teksti sisaldavad plakatid, raamatud ja lehed, tuvastamist videopildist [111], kuid usutavasti ei ole see RangeForce sisseastumiseksami algversiooni jaoks äärmiselt vajalik lisafunktsioon ja võib pigem süsteemi muuta asjatult tundlikuks.

Proovitud peatükis X.

## Muu

Jälgides IP-aadresse, millelt sisseastumiseksamit lahendatakse, on võimalik välistada eksami lahendamise teenus [116]. Nimelt, kui sisseastumiseksamit lahendab ühelt ja samalt IP-aadressilt mitu erinevat kandidaati, võib tegemist olla juhtumiga, kus pakutakse teenust eksami sooritamiseks. Teisalt ei ole võimalik konkreetset IP-aadressi blokeerida, kuna tegemist võib olla ka situatsiooniga, kus kandidaadid lahendavad testi ühes ja samas avalikus internetipunktis, nagu näiteks raamatukogu, ülikool või ühiselamu. Korduvate IP-aadresside puhul on võimalik kandidaadid märgistada ja testimistingimusi vestlusvoorus täpsustada.

Võimalik on analüüsida ka testi sooritamiseks kulunud aega. Kui see on liiga lühike, oli ülesanne tõenäoliselt enne teada ja läbi lahendatud.

Honey pot

# Sobiv süsteem/lahendus

asd

1. Pidev: Süsteemi töös ei tohiks esineda nii pikki pause, et võimaldada olukord, kus toimub kehastusrünnak ehk eksamit või selle osa sooritab eksaminandi eest variisik.
2. Kasutatavus: Süsteem ei tohiks segada kasutaja tööjärge, küsides temalt pidevalt aktiivset autentimist, ega lõpetada tööd iga pidevautentimises esineva väikse kõrvalekalde peale.
3. Turvalisus: Multimodaalne, kombineeritud. Pidev/perioodiline kasutajatuvastus.
4. Andmete turvalisus: Biomeetrilised andmed ei tohi lekkida.
5. Maksumus: Süsteem peaks olema implementeeritav käepäraste standartsete vahenditega, nagu personaalarvuti, veebikaamera, klaviatuur, hiir, mille olemasolu või ostmist võib kasutajalt eeldada.
6. Jõudlus: Videovoo pidev ülekanne serveripoolele koormab ühendust. Parem edastada perioodiliselt pildistatud kaadreid ja analüüsida neid, sest kui ajaraam on piisavalt väike, ei jõua midagi kriitilist juhtuda.

Süsteem võiks anda märku, kui kasutaja nägu kaob kaadrist või kui silmad pole pikemat aega ekraanile fokusseerunud.

Kindlasti ei tohiks eksaminandilt nõuda eririistvara, nagu näiteks autonoomse järelevalveroboti [117], ostmist.

Mitte platvormispetsiifiline.

Usalduskvoot [23]

Kui tuvastus toimub serveripoolel, on klientseadme töökoormus minimaalne [23].

ustrial research. Some of them are mentioned in Section 2 . We identified the following six dimensions for our analysis. •Security : how much it is difficult for impostors to game the system and impersonate a student. •Usability : how much the system disturbs the normal student’s activity to ask specific interactions for recognition purposes. •Efficiency : how much time is required from the system to per- form and return a recognition response. •Long-Term Stability : how much time the biometrics remain stable for the purpose of authentication. •Device - Agnosticism : the ability of the system to work across various types of device. •Interaction-Agnosticism : the ability of the system to detect and authenticate students during different types of interaction [23]

# Kokkuvõte

Kasutatud kirjandus

[1] “DevOps Glossary English-Estonian.” .

[2] “e-Teatmik: IT ja sidetehnika seletav sõnaraamat.” [Online]. Available: http://vallaste.ee/. [Accessed: 03-Apr-2018].

[3] “What is an LMS. What LMS means. Definition of a Learning Management System.” [Online]. Available: https://www.easy-lms.com/help/lms-knowledge-center/what-is-an-lms/item10182. [Accessed: 03-Apr-2018].

[4] IMS Global Learning Consortium, “Learning Tools Interoperability.” [Online]. Available: https://www.imsglobal.org/activity/learning-tools-interoperability. [Accessed: 12-Feb-2018].

[5] A. M. Kaplan and M. Haenlein, “Higher education and the digital revolution: About MOOCs, SPOCs, social media, and the Cookie Monster,” *Bus. Horiz.*, vol. 59, no. 4, pp. 441–450, Jul. 2016.

[6] “MOOCid | Tartu Ülikool.” [Online]. Available: https://www.ut.ee/et/oppimine/moocid. [Accessed: 03-Apr-2018].

[7] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 2014, pp. 1701–1708.

[8] Y. Matsuyama, M. Shozawa, and R. Yokote, “Brain signal׳s low-frequency fits the continuous authentication,” *Neurocomputing*, vol. 164, pp. 137–143, Sep. 2015.

[9] V. Kiisk, “Spektroskoopia alused (loengukonspekt).” Tartu, 2017.

[10] “Elektroentsefalograafia | Haiguste ABC - Kliinik.ee.” [Online]. Available: https://www.kliinik.ee/haiguste\_abc/elektroentsefalograafia/id-292. [Accessed: 03-Apr-2018].

[11] “Tervisenõustamise keskkond - Kliinik.ee.” [Online]. Available: https://www.kliinik.ee/. [Accessed: 03-Apr-2018].

[12] W. Louis, M. Komeili, and D. Hatzinakos, “Continuous authentication using One-Dimensional Multi-Resolution Local Binary Patterns (1DMRLBP) in ECG biometrics,” *IEEE Trans. Inf. Forensics Secur.*, 2016.

[13] “Elektrokardiograafia | Haiguste ABC - Kliinik.ee.” [Online]. Available: https://www.kliinik.ee/haiguste\_abc/elektrokardiograafia/id-293. [Accessed: 03-Apr-2018].

[14] “What is equal error rate (EER)? Webopedia Definition.” [Online]. Available: https://www.webopedia.com/TERM/E/equal\_error\_rate.html. [Accessed: 04-Apr-2018].

[15] M. Langemets and Eesti Keele Instituut., *Eesti keele seletav sõnaraamat*. Eesti Keele Sihtasutus, 2009.

[16] I. Traoré, Y. Nakkabi, S. Saad, B. Sayed, J. D. Ardigo, and P. M. De Faria Quinan, “Ensuring online exam integrity through continuous biometric authentication,” in *Information Security Practices: Emerging Threats and Perspectives*, 2017.

[17] J. Daugman, “How Iris Recognition Works,” in *The Essential Guide to Image Processing*, Elsevier, 2009, pp. 715–739.

[18] V. Korrovits and H. Käämbre, “Inglise-eesti füüsika sõnaraamat.” [Online]. Available: http://www.keeleveeb.ee/dict/speciality/physics\_enet/. [Accessed: 03-Apr-2018].

[19] “ÕIS.” [Online]. Available: https://ois2.ttu.ee/uusois/uus\_ois2.tud\_leht. [Accessed: 26-Mar-2018].

[20] “Küberkaitse.” [Online]. Available: https://www.ttu.ee/teaduskond/infotehnoloogia-teaduskond/sisseastujale-34/magistriope-50/kuberkaitse-2/. [Accessed: 26-Mar-2018].

[21] “Küberkaitse.” [Online]. Available: https://www.ttu.ee/sisseastujale/magistriope-2/23289/sisseastumiskatsed/lisainfo/kuberkaitse-5/. [Accessed: 26-Mar-2018].

[22] “Rangeforce.” [Online]. Available: https://rangeforce.com/home. [Accessed: 26-Mar-2018].

[23] G. Fenu, M. Marras, and L. Boratto, “A multi-biometric system for continuous student authentication in e-learning platforms,” *Pattern Recognit. Lett.*, Apr. 2017.

[24] N. L. Clarke, P. Dowland, and S. M. Furnell, “e-Invigilator: A Biometric-Based Supervision System for e-Assessments,” in *IInternational Conference on nformation Society (i-Society), 2013*, 2013, p. 5.

[25] A. Amigud, J. Arnedo-Moreno, T. Daradoumis, and A.-E. Guerrero-Roldan, “Using Learning Analytics for Preserving Academic Integrity,” *Int. Rev. Res. Open Distrib. Learn.*, 2017.

[26] U. K. Mothukuri, S. Jain, and V. Muralidharan, “Invigilated online assessment: Various ways to minimize unauthorized help,” in *2012 IEEE Symposium on E-Learning, E-Management and E-Services, IS3e 2012*, 2012, pp. 35–38.

[27] M. C. Carlisle and L. C. Baird, “Design and use of a secure testing environment on untrusted hardware,” in *Proceedings of the 2007 IEEE Workshop on Information Assurance, IAW*, 2007.

[28] “Model Behavior.”

[29] M. Lilley, J. Meere, and T. Barker, “Remote Live Invigilation: A Pilot Study,” *J. Interact. Media Educ.*, vol. 2016, no. 1, Jan. 2016.

[30] “Eyes on Integrity A Comparative Look at Online Proctoring Models.”

[31] “Deliver your exam :: Pearson VUE.” [Online]. Available: https://home.pearsonvue.com/Test-Owner/Deliver-your-exam/Testing-outside-a-test-center.aspx. [Accessed: 12-Feb-2018].

[32] N. Mirza and E. Staples, “Webcam as a New Invigilation Method: Students’ Comfort and Potential for Cheating,” *J. Nurs. Educ.*, vol. 49, no. 2, pp. 116–119, 2010.

[33] S. Jose, “Online Proctoring is Trending: Here is All You Should Know About It.” [Online]. Available: http://blog.talview.com/a-complete-guide-to-online-remote-proctoring. [Accessed: 09-Feb-2018].

[34] “RPNow Online Proctoring - Secure Testing. Anytime. Anywhere.” [Online]. Available: http://www.softwaresecure.com/product/remote-proctor-now/. [Accessed: 12-Feb-2018].

[35] “Online Remote Proctoring - Talview.” [Online]. Available: https://www.talview.com/online-remote-proctoring/. [Accessed: 09-Feb-2018].

[36] “About Talview - Online Video Interview Platform.” [Online]. Available: https://www.talview.com/about/. [Accessed: 10-Feb-2018].

[37] “Frequently Asked Questions - Proview.” [Online]. Available: https://staging.proview.io/faq-main/. [Accessed: 12-Feb-2018].

[38] A. Babu, “Talent bazaar on Talview,” *Bus. Stand. News*, p. 25, Jan. 2015.

[39] “Online Examination Software - Talview.” [Online]. Available: https://www.talview.com/online-examination-software/. [Accessed: 10-Feb-2018].

[40] “Customers - Talview.” [Online]. Available: https://www.talview.com/clients/. [Accessed: 10-Feb-2018].

[41] “Remote Proctor PRO FAQ - Secure Testing. Anytime. Anywhere.” [Online]. Available: http://www.softwaresecure.com/remote-proctor-pro-faq/. [Accessed: 10-Feb-2018].

[42] “Remote Proctor Pro - Product Data Sheet.” 2008.

[43] “Purchase Remote Proctor Device.” [Online]. Available: https://www.remoteproctoradmin.com/buyrp/. [Accessed: 10-Feb-2018].

[44] “Amazon.com: SecureExam Remote Proctor: Computers &amp; Accessories.” [Online]. Available: https://www.amazon.com/Software-Secure-SRP5702-Rev-1-0/dp/B009XYBPLW. [Accessed: 12-Feb-2018].

[45] “A TEST OF INTEGRITY: REMOTE PROCTORING IN AN ONLINE CLASS,” *J. Bus. Adm. Online*, vol. 9, no. 2, 2010.

[46] “PSI Services LLC Acquires Remote Proctoring Pioneer Software Secure, Inc. | Business Wire,” *Business Wire*, 2017.

[47] “LTI and Moodle - MoodleDocs.” [Online]. Available: https://docs.moodle.org/34/en/LTI\_and\_Moodle. [Accessed: 12-Feb-2018].

[48] “PSI | Platform | RPNow.” [Online]. Available: https://www.psionline.com/en-gb/platforms/rpnow/. [Accessed: 12-Feb-2018].

[49] “RPNow Quick Demo - softwaresecure.” [Online]. Available: https://softwaresecure.wistia.com/medias/tgkldasdqi. [Accessed: 12-Feb-2018].

[50] “PSI | Education | Clients.” [Online]. Available: https://wwwdemo.psionline.com/en-gb/education/clients/. [Accessed: 12-Feb-2018].

[51] “Pearson VUE Integrated Platform. Flexible testing options with one streamlined system.”

[52] “Microsoft Online Proctored (OP) Exam | Microsoft Learning.” [Online]. Available: https://www.microsoft.com/en-us/learning/online-proctored-exams.aspx. [Accessed: 12-Feb-2018].

[53] “Riigieksami\_vaatlusjuhend\_2017.”

[54] J. D. Woodward, C. Horn, J. Gatune, and A. Thomas, “RAND Public Safety and Justice Biometrics A Look at Facial Recognition.”

[55] I. Martinovic, K. Rasmussen, M. Roeschlin, and G. Tsudik, “Authentication Using Pulse-Response Biometrics,” *Commun. ACM*, vol. 60, no. 2, 2017.

[56] I. Traore and A. A. E. Ahmed, *Continuous authentication using biometrics : data, models, and metrics*. Information Science Reference, 2012.

[57] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar, “User identity verification via mouse dynamics,” *Inf. Sci. (Ny).*, vol. 201, pp. 19–36, 2012.

[58] D. Coffin, “Two-Factor Authentication,” in *Expert Oracle and Java Security*, Berkeley, CA: Apress, 2011, pp. 177–178.

[59] P. Bours, “Continuous keystroke dynamics: A different perspective towards biometric evaluation,” 2012.

[60] J. Rose, Y. Liu, and A. Awad, “Biometric Authentication Using Mouse and Eye Movement Data,” 2017.

[61] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep Face Recognition.”

[62] Y. Sun, D. Liang, X. Wang, and X. Tang, “DeepID3: Face Recognition with Very Deep Neural Networks,” Feb. 2015.

[63] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823.

[64] Y. Xu, T. Price, J.-M. Frahm, and F. Monrose, “Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos,” in *Proceedings of the 25th USENIX Security Symposium*, 2016.

[65] N. Erdogmus and S. Marcel, “Spoofing Face Recognition With 3D Masks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[66] Y. Li, Y. Li, Q. Yan, H. Kong, and R. H. Deng, “Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication.”

[67] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” 2010.

[68] A. Fayyoumi and A. Zarrad, “Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems,” vol. 4, pp. 5–12, 2014.

[69] X. Li, J. Li, L. Liu, and J. Xu, “Face pose estimate technology and its application in video invigilation,” in *2nd International Workshop on Education Technology and Computer Science, ETCS 2010*, 2010, vol. 2, pp. 102–105.

[70] “e-Residency – New Digital Nation.” [Online]. Available: https://e-resident.gov.ee/. [Accessed: 23-Mar-2018].

[71] “AKIT - Andmekaitse ja infoturbe leksikon.” [Online]. Available: http://akit.cyber.ee/term/5998-iris-recognition. [Accessed: 23-Mar-2018].

[72] “Iris Recognition.”

[73] L. C. F. Araujo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu-Uti, “User authentication through typing biometrics features,” *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 851–855, Feb. 2005.

[74] S. Mondal and P. Bours, “Person Identification by Keystroke Dynamics Using Pairwise User Coupling,” *IEEE Trans. Inf. Forensics Secur.*, 2017.

[75] J. V. Monaco, N. Bakelman, S.-H. Cha, and C. C. Tappert, “Developing a Keystroke Biometric System for Continual Authentication of Computer Users,” in *2012 European Intelligence and Security Informatics Conference*, 2012, pp. 210–216.

[76] J. Roth, X. Liu, and D. Metaxas, “On continuous user authentication via typing behavior,” *IEEE Trans. Image Process.*, 2014.

[77] H. Saevanee and P. Bhattarakosol, “Authenticating User Using Keystroke Dynamics and Finger Pressure,” in *2009 6th IEEE Consumer Communications and Networking Conference*, 2009, pp. 1–2.

[78] H. Saevanee and P. Bhatarakosol, “User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device,” in *2008 International Conference on Computer and Electrical Engineering*, 2008, pp. 82–86.

[79] Y. Sun, H. Ceker, and S. Upadhyaya, “Shared keystroke dataset for continuous authentication,” in *8th IEEE International Workshop on Information Forensics and Security, WIFS 2016*, 2017.

[80] I. Deutschmann, P. Nordstrom, and L. Nilsson, “Continuous Authentication Using Behavioral Biometrics,” *IT Prof.*, vol. 15, no. 4, pp. 12–15, Jul. 2013.

[81] S. Mondal and P. Bours, “A study on continuous authentication using a combination of keystroke and mouse biometrics,” *Neurocomputing*, vol. 230, pp. 1–22, Mar. 2017.

[82] S. Mondal and P. Bours, “Continuous Authentication using Mouse Dynamics.”

[83] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, “Biometric Authentication Using Mouse Gesture Dynamics,” *IEEE Syst. J.*, vol. 7, no. 2, pp. 262–274, Jun. 2013.

[84] M. Sharif, T. Faiz, and M. Raza, “Time signatures - an implementation of Keystroke and click patterns for practical and secure authentication,” in *2008 Third International Conference on Digital Information Management*, 2008, pp. 559–562.

[85] “Multi-factor Authentication Using Gesture Biometrics - Biometric Signature ID.” [Online]. Available: https://www.biosig-id.com/. [Accessed: 04-Mar-2018].

[86] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous Verification Using Multimodal Biometrics,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 687–700, Apr. 2007.

[87] NIST report to the United States Congress, “SUMMARY OF NIST STANDARDS FOR BIOMETRIC ACCURACY, TAMPER RESISTANCE, AND INTEROPERABILITY EXECUTIVE SUMMARY Large Scale Testing,” 2002.

[88] X. Liu, L. Kong, Z. Diao, and P. Jia, “Line-scan system for continuous hand authentication,” 2017.

[89] “Fujitsu PalmSecure - Fujitsu Global.” [Online]. Available: http://www.fujitsu.com/global/solutions/business-technology/security/palmsecure/. [Accessed: 11-Mar-2018].

[90] “PalmSecure Mouse.” .

[91] “AKIT - Andmekaitse ja infoturbe leksikon.” [Online]. Available: http://akit.cyber.ee/term/12784-soft-biometrics. [Accessed: 09-Mar-2018].

[92] A. K. Jain, S. C. Dass, and K. Nandakumar, “Can soft biometric traits assist user recognition?”

[93] K. Niinuma, U. Park, and A. K. Jain, “Soft Biometric Traits for Continuous User Authentication,” *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 4, pp. 771–780, Dec. 2010.

[94] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras, “Towards a continuous biometric system based on ECG signals acquired on the steering wheel,” *Sensors (Switzerland)*, 2017.

[95] S. Vhaduri and C. Poellabauer, “Wearable device user authentication using physiological and behavioral metrics,” in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–6.

[96] C. D. Holland and O. V. Komogortsev, “Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 2115–2126, Dec. 2013.

[97] R. J. Leigh and D. S. Zee, *The Neurology of Eye Movements*. Oxford University Press, 2015.

[98] Y. Cheung and Q. Peng, “Eye Gaze Tracking With a Web Camera in a Desktop Environment,” *IEEE Trans. Human-Machine Syst.*, vol. 45, no. 4, pp. 419–430, Aug. 2015.

[99] J. San Agustin, H. Skovsgaard, J. P. Hansen, and D. W. Hansen, “Low-cost gaze interaction,” in *Proceedings of the 27th international conference extended abstracts on Human factors in computing systems - CHI EA ’09*, 2009.

[100] H. Skovsgaard, J. S. Agustin, S. A. Johansen, J. P. Hansen, and M. Tall, “Evaluation of a remote webcam-based eye tracker,” in *Proceedings of the 1st Conference on Novel Gaze-Controlled Applications - NGCA ’11*, 2011.

[101] D. C. Niehorster, T. H. W. Cornelissen, K. Holmqvist, I. T. C. Hooge, and R. S. Hessels, “What to expect from your remote eye-tracker when participants are unrestrained,” 2017.

[102] D. Bäck, “Neural Network Gaze Tracking using Web Camera,” Linköpings tekniska högskola (Institutionen för medicinsk teknik), 2005.

[103] A. Boehm *et al.*, “SAFE: Secure authentication with Face and Eyes,” in *2013 International Conference on Privacy and Security in Mobile Systems, PRISMS 2013 - co-located with Global Wireless Summit*, 2014.

[104] Bharath S Sirur and Shankar Pendse, “Gaze driven architecture: Adding new dimensions to level of security in computers,” in *2010 3rd International Conference on Computer Science and Information Technology*, 2010, pp. 200–205.

[105] W. Sewell and O. Komogortsev, “Real-Time Eye Gaze Tracking With an Unmodified Commodity Webcam Employing a Neural Network,” in *Proceedings of ACM Conference on Human Factors in Computing Systems (CHI)*, 2010.

[106] “EnumDisplayMonitors function (Windows).” [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/dd162610(v=vs.85).aspx. [Accessed: 24-Mar-2018].

[107] “EnumDisplayDevices function (Windows).” [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/dd162609(v=vs.85).aspx. [Accessed: 24-Mar-2018].

[108] “xrandr - ArchWiki.” [Online]. Available: https://wiki.archlinux.org/index.php/xrandr. [Accessed: 24-Mar-2018].

[109] “Respondus.” [Online]. Available: https://www.respondus.com/. [Accessed: 11-Mar-2018].

[110] “Safe Exam Browser - About.” [Online]. Available: https://safeexambrowser.org/about\_overview\_en.html. [Accessed: 11-Mar-2018].

[111] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, “Automated Online Exam Proctoring,” *IEEE Trans. Multimed.*, 2017.

[112] “Anti-VM and Anti-Sandbox Explained - Cyberbit.” [Online]. Available: https://www.cyberbit.com/anti-vm-and-anti-sandbox-explained/. [Accessed: 12-Mar-2018].

[113] “How Malware Detects Virtualized Environment (and its Countermeasures),” 2016. [Online]. Available: http://resources.infosecinstitute.com/how-malware-detects-virtualized-environment-and-its-countermeasures-an-overview/. [Accessed: 12-Mar-2018].

[114] C. Jämthagen, M. Hell, and B. Smeets, “A Technique for Remote Detection of Certain Virtual Machine Monitors,” Springer, Berlin, Heidelberg, 2012, pp. 129–137.

[115] M. Noorafiza, H. Maeda, T. Kinoshita, and R. Uda, “Virtual machine remote detection method using network timestamp in cloud computing,” in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 2013, pp. 375–380.

[116] J. Moten, A. Fitterer, E. Brazier, J. Leonard, and A. Brown, “Examining online college cyber cheating methods and prevention measures,” *Electron. J. e-Learning*, 2013.

[117] W. A. Rosen and M. E. Carr, “An autonomous articulating desktop robot for proctoring remote online examinations,” in *2013 IEEE Frontiers in Education Conference (FIE)*, 2013, pp. 1935–1939.

Lisa 1 –