E-valimiste realiseerimisvõimaluste analüüs

Helger Lipmaa
helger@tml.hut.fi
http://www.tml.hut.fi/~helger

Oleg Mürk
olegm@ut.ee
http://www.ut.ee/~olegm

9. aprill 2001. a.

Sisukord

Kokkuvõte

Eesti Vabariik on olnud sageli esirinnas erinevate “e-teenuste” pakkumisel, kus tavaline, pabereid nõudev teenus (nagu näiteks panganduses klientide teenindamine) on Interneti kasutamise läbi põhjalikult reformeeritud. Kuna enamus saadud kogemusi on positiivsed ja tõstnud Eesti prestiiži, on nii tavakodanikud kui ka vabariigi valitsus huvitatud järjest uute e-teenuste kasutusele võtust.

Viimase paari kuu jooksul on kerkinud päevakorda Interneti kaudu *valimiste* (nn e-valimiste) korraldamine juba 2002. aastal. Käesoleva materjali eesmärgiks on anda lühiülevaade e-valimiste korraldamise võimalikkusest ning selle juures tekkivatest probleemidest. Me selgitame, miks turvaliste e-valimiste korraldamine on tehniliselt oluliselt raskem, kui näiteks e-panganduse või digiallkirjade korraldamine.

Kuigi antud raporti põhiresultaat on negatiivne (2002. aastal üldriiklike e-valimiste korraldamine on olemasoleva tehnoloogia juures utoopiline), soovitame me antud teema uurimist jätkata. Me peame ka võimalikuks vähema tähtsusega valimiste (näiteks kohalike omavalitsuste valimiste) pidamist nelja kuni kaheksa aasta jooksul.

Me rõhutame, et digiallkirja seaduse ettevalmistamine võttis aega umbes kolm aastat. E-valimiste korraldamiseks kuluv ettevalmistusaeg on vähemalt sama pikk, kui mitte pikem. Kuigi e-valimiste korraldamisega võib Eesti Vabariik võita endale nö “plusspunkte”, on moraalne kahju halvasti ette valmistatud e-valimistest oluliselt suurem nii rahvusvaheliselt kui ka siseriiklikult.

Antud raport on põhiliselt tehniline, ning meie järeldused e-valimiste korraldamise “võimatuse” kohta on puhttehnoloogilised.

Raport on eeskätt mõeldud kasutamiseks Eesti Vabariigi justiitsministeeriumis ning teistes ametiasutustes. Sellest on tingitud ka raporti suunitlus. Samas ei sisalda raport salajast infot. Raportit võib vabalt levitada tingimusel, et levitamine toimub täies ulatuses.

Raporti autorid on eraisikud, kelle ametikohti on mainitud vaid hõlpsama kontakteerumise võimaldamiseks. Nende töökohad ei oma mingeid õigusi ega kohustusi, mis on seotud selle raportiga. Raport väljendab vaid töö autorite isiklikke veendumusi.

Raport valmis limiteeritud aja jooksul, ja teda tuleb käsitleda kui sellist. Palju paremat tulemust on ilmselgelt võimalik saavutada suurema töömahu korral. Seetõttu ei garanteeri autorid raporti sajaprotsendilist tõele vastavust.

Helger Lipmaa on Helsinki Tehnoloogiaülikooli vanemteadur (alates 2001. augustist, professor). Avaldanud mitmeid teaduslikke artikleid krüptograafiast.

Oleg Mürk on Tartu Ülikooli üliõpilane. Tema 2000. aastal kirjutatud semestritöö e-valimistest võitis Eesti Teaduste Akadeemia auhinna.

Peatükk 1

Sissejuhatus

1.1 E-valimised versus tavalised valimised

E-valimiste all mõtleme käesolevas dokumendis valimisi, mis toimuvad täielikult üle Interneti, ning mille vahendusel saavad valijad hääletada enese poolt valitud arvuti või muu seadme, nagu näiteks mobiiltelefoni, abil üle Interneti. Me käsitleme lühidalt ka muid võimalusi, kus valida saab näiteks spetsiaalselt selleks eraldatud arvutitest koolides ja raamatukogudes (nn "valimiskioskite" kasutamine). Me paneme põhirõhu eelnevas lauses toodud e-valimiste definitsioonile, kuna valimiskioskite kasutamisel langeb ära enamus e-valimistelt oodatud eelistest.

E-valimiste korraldamise poolt tuuakse tavaliselt välja järgmised argumendid:

1. *Valijate osaluse tõstmine*. Osa elanikkonnast ei saa või ei taha valimiste nimel valimisteks määratud päevade jooksul valimisjaoskonnas käia. Sellesse rühma kuuluvad nooremad valijad, kes on liiga hõivatud, välismaal reisivad Eesti kodanikud, ning loodetavasti ka vanurid ja puuetega inimesed.

2. *Kasutamismugavus*. (Seotud eelmise punktiga.) E-valimistel oleks valijate poolt tehtav "töö" (sobiva kandidaadi poolt hääletamine) tehtav palju lihtsamalt. Lisaks sellele on võimalik abistada puuetega inimesi, luues neile sobivaid hääletusvahendeid.

3. *Odavus*. Väheneb vajadus palgata spetsiaalseid inimesi ja rentida ruume.

Samas peavad nii riigikogu kui ka kohalike omavalitsuste valimised rahuldama Eesti Vabariigi põhiseaduse [EVP92] paragrahvides 60 ja 156 väljendatud omadusi:

1. Valimised peavad olema *üldised ja ühetaolised*: kõigile valijatele peab olema garanteeritud ühesugune valimisõigus, sõltumatult näiteks nende haridustasemest või jõukusastmest. Kõik valijad peavad saama hääletada, ükski hääl ei tohi minna arvestusse kahekordselt.

2. Valimised peavad olema *salajased*: iga inimese hääletustulemused peavad jääma vaid tema enda teada. Muuhulgas peab kehtima tugevam omadus, *valimisvabadus*: "valimised on vabad, kui hääletamine toimub ilma sunni ja lubamatu surveavaldamiseta valijale" (viide: http://www.just.ee/pohiseadus/5riigikogu.htm). Sealhulgas peaks olema välistatud häälte ostmine.

Hetkel läbi viidavad valimised rahuldavad (kuigi mitte täielikult) mõlemat toodud nõuet. Valimised on salajased, kuna valija kasutab hääletuseks anonüümset meediat (valget paberilehte). Valimised on üldised ja ühetaolised, kuna valimisjaoskondades peetakse arvet juba hääletanud kodanike üle. Nagu öeldud, ei ole kumbki nõue täidetud täielikult, kuid siiski küllaltki suure kindlusega. Nii näiteks võib valijate anonüümsust rikkuda hiljem valimissedelitele käekirja- või DNA-analüüsi tehes, kuid see on küllaltki kulukas. Lisaks sellele ei ole võimalik antud analüüse tegemist hoida salajas. Täielikku ühetaolisust välistab aga nõue, et valijad peavad valimisteks viibima ettenähtud valimisjaoskonnas. Paljudele valijatele on selle nõude täitmine kas liiga tülikas (näiteks puuetega inimestele) või kulukas.

Krüptograafiliselt turvalised e-valimised lubaksid vähemalt osaliselt üle saada nii täieliku salajasuse kui ka (hüpoteetiliselt) ühetaolisuse puudumisest. Kahjuks ei ole tegu aga "imerohuga". Järgnevas tuleb välja, et e-valimiste korral on salajasus ja ühetaolisus vastandlikud omadused: valijate parem anonüümsus vähendab ühetaolisust, ja vastupidi. Mainitud tasakaalu põhiliseks põhjuseks on *valija arvuti turvamise keerukus ning kulukus*.

E-valimiste turvaliseks läbiviimiseks ei piisa samast turvatasemest, mis on näiteks e-panganduses, kuna valimiste korral sõltub sageli ka alla kümne valija otsusest valimiste tulemus. Viimane aga mõjutab olulisel määral riigi saatust järgneva nelja aasta jooksul. *Seetõttu võib e-valimiste vastu oodata tunduvalt argressiivsemaid ründeid kui e-panganduse vastu*, kusjuures ründe objektideks on kas valijate (e-valimissüsteemi klientide) arvutid ning arvutite ja valimiste keskserverite vaheline Internetiühendus.

Kliendi arvuti ebaturvalisus e-panganduse süsteemis mõjutab vaid klienti ennast, kes võib pärast esimesi ebaturvalisuse märke silmates kas loobuda e-panganduse kasutamisest või palgata spetsialist turvaprobleemide lahendamiseks. Internetiühenduse katkemisel võib klient kas ülekande teostamist edasi lükata või

kasutada (ühekordselt) pangakontorite teenuseid. E-panganduse korral võib ka eeldada, et jõukamad inimesed kasutavad turvalisemaid masinaid oma ülekannete sooritamiseks kui vähemjõukad inimesed. E-valimiste korral sellised lahendused ning eeldused ei aita, kuna nad käiksid otseselt vastu ühetaolisuse nõuetele.

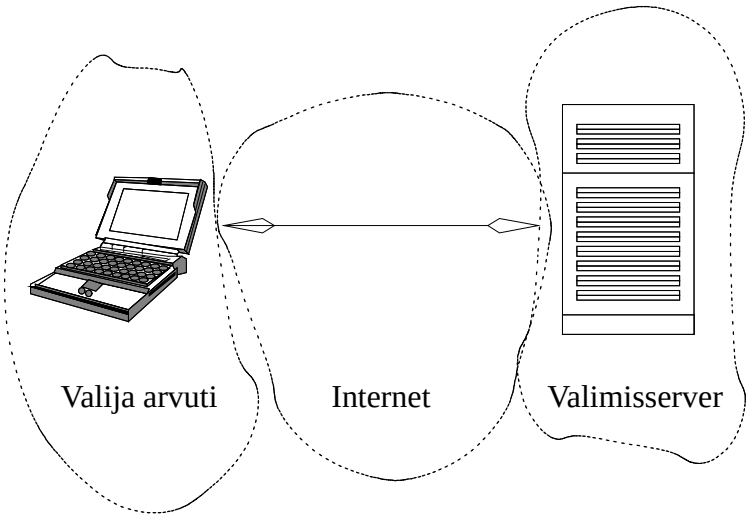
E-valimiste turvalisus mõjutab oluliselt kasutajate usaldust nii valimiste kui ka seda läbiviivate organite, pikemas perspektiivis aga ka demokraatia vastu. Seetõttu on enamus käesolevast raportist pühendatud justnimelt andmeturbe probleemidele. E-valimistega seonduvatest sotsiaalsetest probleemidest ning nende järeldustest annab küllaltki hea ülevaate just hiljuti publitseeritud USA e-valimistealase töörühma mittetehniline raport [Ins01]. Seal toodud järeldused nii tehnilise kui ka sotsiaalse poole pealt on enamvähem ühilduvad meie järeldustega. Suuremad erinevused meie järeldustes tulenevad juba olemasolevast või loodavast tehnilisest infrastruktuurist.

Järgnevas käsitleme lähemalt e-valimiste infosüsteemi erinevate komponentide turvaprobleeme.

1.2 E-valmiste korraldamise erinevad aspektid

E-valimiste edukaks kordaminekuks on vaja mitmete teineteisest enamasti sõltumatute, nii organisatoorsete kui tehniliste, lahenduste tõrgeteta ja sujuvat koostööd. Nagu kõik süsteemid, on ka e-valimiste infosüsteem täpselt sama tugev kui tema kõige nõrgem koostisosa. Seega tuleb e-valimiste ettevalmistusprotsessi jooksul tähelepanu pöörata kõikide e-valimises vaja minevate üksuste turvalisele ja töökindlale funktsioneerimisele. Muuhulgas peab süsteemi kõikide osade tegevus olema spetsifitseeritud, ning kõigi osade tegevuse spetsifikatsioonidele vastavus verifitseeritav. Ainult e-valimiste süsteemi avatus ja verifitseeritavus toob süsteemile ka kõikide osapoolte (riik, hääletajad, rahvusvaheline üldsus) usalduse.

Vaatleme joonisel 1.1 kujutatud diagrammi, mis aitab selgitada e-valimiste infosüsteemi mõningaid aspekte. Toodud diagramm on ülimalt lihtsustatud, kujutades vaid kolme e-valimiste infosüstemi põhikomponenti: valija ning hääletusjaoskonna arvutit ning nendevahelist ühenduskeskkonda. Kõik diagrammil toodud üksused on erinevate peremeeste “hallata”. Valija arvutit haldab valdaja ise, serverit haldab valimiskomisjon, Interneti “haldajaks” võib aga pidada laiemas laastus kogu inimkonda. Kõiki kolme komponenti (täpsemalt, valija arvutit, valimisservereid ning valija arvuti ja serveri vahelist võrguliiklust) peab turvama eraldi ning erinevate meetodite abil, meeles pidades et ahel on sama nõrk kui kõrge nõrgem lüli. Ei ole *ühtset ja lihtsat* lahendust terve infosüsteemi



Joonis 1.1: E-valimiste põhikomponendid (lihtsustatud joonis).

kaitsmiseks: ainuke võimalus on turvata kõiki komponente eraldi.

E-valimiste korralikuks toimimiseks peab tegema (pisut lihtsustatult) järgmised eeldused:

- Valija arvuti (nii riist- kui tarkvara) peab töötama tõrgeteta ja spetsifikatsioonidele vastavalt. Arvutis ei tohi olla viiruseid, Trooja hobuseid, ega muud pahatahtlikku tarkvara.
- Samad nõued, aga veelgi tugevamalt rõhutatult, peavad kehtima valimisserveri kohta, kuna viimane kogub tuhandete valijate hääli.
- Hääle liikumine digitaalkujul valija arvutist valimisserverisse peab olema turvaline. Sealjuures peab hääl ise olema salajane (isegi valimisserver ei tohi teada saada, kelle poolt antud valija hääletas) [EVP92, paragrahv 60].
- Valimisserverite ja/või valijate arvutite (või teiste ühenduseks vajalike arvutite) vastu saab rakendada *teenusetõkestamise* ründeid (*Denial of Service*), mis seisneb võrgu mahutatavuse ülekoormamises. Teenusetõkestamise rünne võib olla hajus (rakendatud korraga tuhandete erinevate arvutite poolt).

- Valijal peab olema *hääletamisvabadus*: hääletamise protsess peab tegema võimatuks häälte ostmise ja valijate (endale sobiva kandidaadi poolt) hääletama sundimise.

Mainitud turvaprobleemide täielikku lahendamist on praktiliselt võimatu garanteerida. Selgitame seda lühidalt. Valija arvutiks on tavaliselt Microsoft Windowsi keskkonnas töötav koduarvuti. Kõik muud lahendused, nagu näiteks personaalsed turvakeskkonnad, on võimalikud, kuid neid kasutatakse vähe ning nende omandamine valijate poolt puhtalt valimiste läbiviimiseks on ebamõistlik: meenutagem, et e-valimiste motivatsiooniks on hääletamise mugavuse tõstmine ning valimisprotsessi kulude vähendamine. Tavaline koduarvuti sisaldab tõenäoliselt peale operatsioonisüsteemi ka kontoritarkvara, mänge, ning võimalik, et ka viiruseid. Isegi usaldades, et operatsioonisüsteemi ja muu tarkvara autorid ei ole modifitseerinud tarkvara nii, et viimases on sees e-valimisi segavad salaluugid, on *võimatu* garanteerida, et salaluuke pole tarkvarasse tekitanud keegi teine. Võib esineda ka tahtmatuid vigu, mis mõjutavad negatiivselt arvuti töökindlust.

Kõige lihtsam valimismeetod (valija täidab veebilehitsejas teatava veebilehe, vajutades sobiva kandidaadi nimele, ning saadab selle serverile) on ebaturvaline väga mitmetel, küllalt triviaalsetel, põhjustel. Sellisel juhul võib näiteks kasutaja suunata (ilma tema teadmata) libaserveri poole, kes täidab muidu kõiki pärisserveri funktsioone, kuid jätab meelde ka hääle (halvimal juhul hääletab kellegi teise poolt).

Valimisserveritega on olukord mõnevõrra lihtsam, kuna siin võib vabariigi valimiskomisjon tellida $1 \ldots 10$ *turvalist* arvutid kõrgemate turvastandardite järgi sertifitseeritud riistvara ja tarkvaraga. Kuid iga sellise arvuti hind on mitmeid kordi kõrgem tavalise serveri hinnast. Lisaks sellele võib serveri turvalisus olla väiksem lubatust, kuna kas tarnijakompanii või mõni serveri haldajatest/tehnikutest on ära ostetud ühe kindla erakonna poolt.

Valimiste sundimatuse tagamiseks peab olema võimalus valimistel privaatselt hääli tagasi võtta: tühistada oma eelmine hääl ning hääletada uuesti, ilma et häälte tagasivõtmist oleks võimalik kontrollida. Selleks on vaja teatud administratiivsete ja krüptograafiliste meetodite kooslust; sajaprotsendiliselt on ka seda probleemi võimatu lahendada.

Teenusetõkestamise rünnetes ummistatakse kas valija ja valimisserveri vaheline Internetiühendus, või arvutid ise, saates neile nii palju informatsiooni, et arvutid ei ole võimelised seda töötlema. Rünnet võivad rakendada nii legitiimsed valijad kui ka kõik teised: sealjuures võivad ründajad pärit olla meie planeedi suvaliselt mandrilt. Rünnet on võimalik pehmendada (kuid mitte vältida!)

suurema mahutuvusega Internetiühenduste ning suurema protsessorikiiruse ja mälumahuga arvutite muretsemise teel. Samas võimaldab suurema mahtuvusega Internetiühendus ka ründajatel teostada efektiivsemaid ründeid, rääkimata selle lahenduse kallidusest. Hajusrünnete vastu, kus ründajateks on potentsiaalselt tuhanded erinevad arvutid, tänapäeval kaitsevahendid puuduvad.

Kõiki eelmainitud aspekte käsitleme lähedalt, aga lühidalt, järgnevates peatükkides. Põhjuseks on, nagu öeldud, nende probleemide (suures osas) lahendamatus. Me toome välja üldised nõuanded, mida peaks turvataseme tõstmiseks järgima. Samas ei ole need nõuanded täiuslikud ning vajavad kindlasti edasist uurimistööd nii praktiliselt kui ka teoreetiliselt. (Ka selles osas langeb meie soovitus kokku USA raporti soovitustega [Ins01].) Üheks oluliseks probleemiks on süsteemi turvalisuse hindamise objektiivsete vahendite puudumine. Ainsaks lahendiks on (vähemalt tänapäeval) usaldus oma eriala spetsialistide vastu, kes on auditeerinud süsteemi turvataset ja sellega rahule jäänud.

Nagu juba mainitud, on meie põhijärelduseks see, et kogu süsteem peab olema (ideaalis) verifitseeritav. Nii näiteks peavad kasutajad saama kontrollida soovi korral oma tarkvara autentsust. Samas ei ole paljudel valijatel viimaseks ei oskusi, aega ega vahendeid. Seega, e-valimiste toimumine põhineb suurelt osalt valijate usaldusel teiste inimeste vastu (vt peatükk 2.1).

Samas salajast elektroonilist hääletamist on võimalik realiseerida, kasutades krüptograafilisi protokolle, eeldusel et on olemas turvalised serverid, võrguühendus ning hääletajate arvutid, Nii lahenduste olemasolu, kui ka oma krüptograafilise tagatausta ja huvide tõttu pühendame enamuse käesolevast raportist just sellele temaatikale.

Sissejuhatuse lõpetamiseks selgitame lühidalt e-valimiste turvanõuete täitmise tähtsust. Nii näiteks võib väita, et tavaliste valimiste puhul ei ole valikuvabadus alati täidetud. Tõepoolest, ka Eesti Vabariigi praktikas on esinenud häälte ostmise juhte. Samas on häälte ostmine ja valijate sundimine tavavalimiste puhul kulukas ja vaevaline protsess, mis avastatakse suure tõenäosusega teatud mastaapideni jõudmise korral. Samas e-valimiste korral on rünnete teostamine märgatavalt odavam, ja mis peaasi, anonüümne: vähemalt antud raporti autorid kujutavad selgelt ette automatiseeritud “hääleostmisservereid”.

Arvatavasti kõige ilmekamalt võib aga erinevust tava- ja e-valimiste vahele seletada häälte võltsimise näite varal. Eeldades, et valimiskomisjoni liikmed on usaldatavad (ehk loevad ausalt kokku sedelitel olevad hääled), seisneb tavavalimiste korral häälte võltsimine vanade sedelite uutega asendamises. Seda peab tegema salaja, ja varjatult, ning sellega seosneb suur hulk praktilisi probleeme. (Kujutagem ette plekkmannerguga koristajatädi, kes murrab lahti range valve all

oleva šeifi ja puistab sinna paar tuhat sedelit.) Samas e-valimiste korral tähendab hääle võltsimine vaid mõnede üksikute baitide muutmist kuskil arvutis. Muutjaks võib olla suvaline isik, kellel on vähemalt osaline kontroll kas hääletaja arvuti, valimisserveri või vahepealse Internetiühenduse üle.

Summa summarum, e-valimiste "ründamine" on märksa lihtsamini täide viidavam, kui tavavalimiste "ründamine", ning seetõttu tuleb väga suurt rõhku panna e-valimiste turvapoolele.

Peatükk 2

Üldnõuded

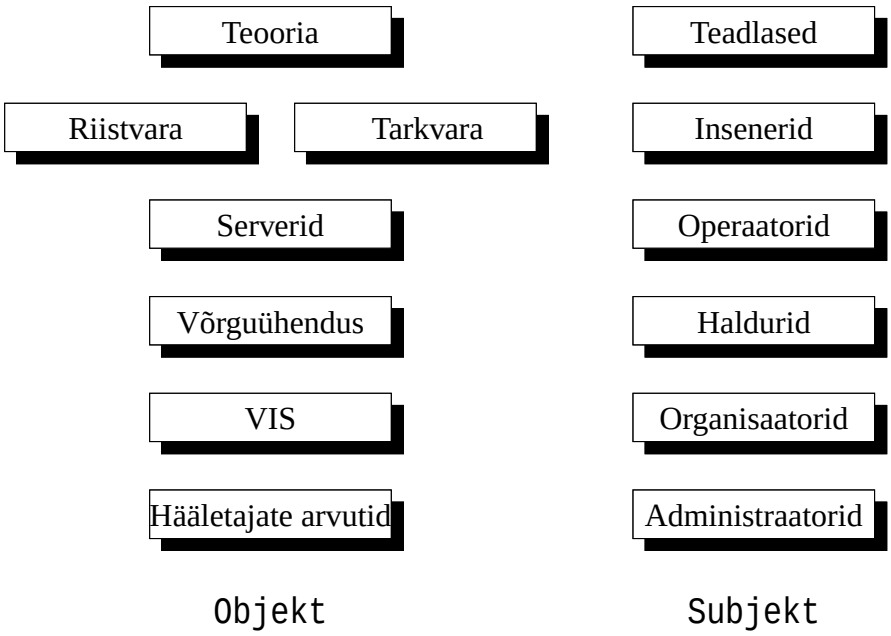
2.1 Usaldusmäära tähtsus

E-valimiste infosüsteem (EVIS) koosneb teatud hulgast *e-valimise serveritest*, mida võib vaadelda koosnevat teatud töökindlast *riistvarast* ning verifitseeritud *tarkvarast*. Peale selle on olemas *hääletajate arvutid*, mis samuti koosnevad riistning tarkvarast. Kogu infosüsteem on ülesehitatud teatud sulamile teoreetilistest baasteadmistest (vt joonis 2.1).

E-valimiste infosüsteemi ehitanud ja haldavaid inimesi nimetame *organisaatoriteks*. Inimesi, kes ehitasid üles ning haldavad konkreetseid servereid nimetame *operaatoriteks*. Inimesi, kes tegelevad hääletajate arvutite korrashoiuga nimetame *administraatoriteks* (valdavalt on administraatoriks valija ise). Inimesi, kes hooldavad võrguühendust, nimetame *halduriteks*. Inimesi, kes ehitasid valmis riistning tarkvara nimetame *inseneridеks*. Lõpuks, teoreetilise baasi autoriteks on *teadlased*.

E-valimiste usaldatavus põhineb seega nii organisaatorite, serverite, hääletajate arvutite, riist- ja tarkvara ning teoreetilise baasi usaldatavusel. Oluline on ka vaatlejate (oma ala ekspertide) kohalolu, kes verifitseerivad süsteemi erinevaid aspekte ning esitavad oma arvamuse (millega võib kaasneda ka vastutus). Nii peaksid erinevad vaatlejad sertifitseerima kasutatavat riist- ja tarkvara, samas kui teised vaatlejad spetsialiseeruvad häältelugemise korrektsuse kontrollile.

Käesolevas tekstis lähtume sellest, et e-valimiste infosüsteem peab olema realiseeritud Internetis asuva teenusena ning saab kasutada üldriikliku *avaliku võtme infrastruktuuri* (PKI) võimalusi. Sealjuures peab igal valijal olema oma avaliku



Joonis 2.1: E-valimiste infosüsteemi peamised komponendid. Joonise paremas servas on toodud isikud, kes on seotud vastavate komponentide leiutamise, ülespaneku või turvamisega, ning kelle vastu peab valijal seega olema vähemalt minimaalne usaldus.

võtme sertifikaat. Märgime, et riiklik PKI peab töötama ka digitaalallkirjaseaduse edukaks rakendamiseks, seega ei ole töötava PKI olemasolu eeldus liiga ebarealistlik. Küll on aga ebarealistlik eeldada üleriikliku PKI teket järgmiseks või ülejärgmiseks aastaks.

Nagu juba eelnevalt mainitud, on usalduse saavutamiseks e-valimiste vastu oluline kogu süsteemi *avatus* ja *verifitseeritavus*: nii EVISi teoreetilised alused kui ka kasutatava tarkvara lähtekood peavad olema kõigile soovijatele nii Eestis kui ka välismaal kättesaadavad. Hääletaja peab ise saama valida tema poolt kasutatavat operatsioonisüsteemi ja riistvaratüüpi: tüüpilised personaalarvutite installatsioonid on ebaturvalised, samas on vähemtüüpiliste OS-ide ja arvutitüüpide (spetsiaalsed personaalsed turvakeskkonnad) kasutamine tavavalija jaoks oluliselt kulukam. Mis kõige olulisem, *hääletaja peab saama ise valida oma soovitud turvaklassi, vastavalt oma usaldusele valimiste organisaatorite, inseneride, e-valimiste tarkvara levitajate, administraatorite ja teiste osapoolte vastu*. Ka need valijad, kellel pole võimalusi kõrgele turvaklassile vastavat riist- ja tarkvara muretseda, peavad saama hääletada. Viimastele peab kindlalt teadvustama, et neil on valida tavaliste valimiste või madala turvatasemega e-valimiste vahel. Madala turvatasemega seotud ohud peavad olema samuti üles loetud.

E-valimiste alguseks peab olema valmis *tasuta* klienditarkvara enamlevinud keskkondadele nagu MS Windows, Mac OS, Linux, PalmOS. Loomulik on ka platvormsõltumatu tarkvara, näiteks kirjutatud Javas, olemasolu. (Viimane oleks kasutajale mugavam, kuid samas ka enamasti oluliselt aeglasem, kui platvormist sõltuv klienditarkvara.) Klienditarkvara levitamine peab toimuma turvaliselt, ehk teisiti, e-valimiste klienditarkvara autentsus peab olema verifitseeritav. Soovitavaks lahenduseks on siin tarkvara mitmekordne digitaalne signeerimine erinevate autoriteetide (näiteks vabariigi presidendi, valimiskomisjoni, õiguskantsleri, erinevate erakondade esindajad) poolt; digitaalallkirjade kehtivuse garanteerimiseks tuleb rakendada nii digitaalallkirja seadust kui ka võimaluse korral muid turvameetodeid.

Rõhutame, et enamus (kui mitte kõik) valijaid on ebakompetentsed oma turvataseme kindlaks määramisel. Kompetentsust ei saa eeldada ei lihttööliselt ega Riigikogu liikmelt. Seega on usaldus spetsialistide vastu vältimatu. Soovi korral peab hääletaja siiski saama nii EVISi serveripoolse kui ka hääletajat teenindava osa riist- ja tarkvara õigsust verifitseerida; viimaseks võib hääletaja soovi korral kutsuda välja enda kulul vastava eksperdi (vaatleja). Valija (või tema poolt palgatud ekspert) peab saama e-valimiste kliendiprogrammi modifitseerida, kas enda turvalisustaseme kasvuks või muudel eesmärkidel. Näiteks võib hääletaja soovida kliendiprogrammi kohandada tema personaalse turvakeskkonna ametlikult mitte-

toetatavale operatsioonisüsteemile (näiteks EPOC või Windows CE).

E-valimiste serveritarkvara peab aktsepteerima neid hääli, mis vastavad oma vormingult eelnevalt avalikustatud spetsifikatsioonile. Siit selgub ka spetsifikatsiooni tähtsus: õigesti edastatud hääled peavad saama arvestatud. Samas peab serveritarkvara oskama toime tulla ka siis, kui servereid teadlikult rünnatakse pahatahtlike programmide poolt. Serveritarkvara ei tohi arvestada vale vorminguga hääli, samuti peab tarkvara kaitsma servereid teenusetõkke (*Denial of Service*) tüüpi rünnete vastu. Teisest küljest, hääletajad peavad saama kontrollida, et nende õigesti vormistatud hääli on arvestatud e-valimiste lõpptulemuste arvutamisel.

2.2 Võimalikud ründed

Käesolevas peatükis kirjeldame võimalikke ründeid EVISi vastu:

- Valija arvutisse sissemurdmine ning tema salajase võtme varastamine või programmide modifitseerimine.
- Korraldajate arvutitesse sissemurdmine.
- Võrguühenduse rikkumine (näiteks ummistamine).
- Korraldajate üleostmine.
- Valijale ei anta võimalust hääletada.
- Valija saadetud häält ei arvestata.
- Lisatakse hääli valimistes mitteosalenud hääletajate nimel.
- Valimistulemuste vale kokkulugemine.

Neist rünnetest enamus on välditavad (või pole üldse defineeritavad) tavaliste valimiste korral, kui valimist toimepanev meeskond ja vaatlejad on usaldatavad.

Üritame järgnevas klassifitseerida valimissüsteemile toimepandavaid ründeid ründe sooritaja järgi, ning toome koheselt ära ka nõuanded, millistel meetoditel neid ründeid vältida saaks. Samal teemal võib lugeda ka ülevaadet [Ins01].

Järgnevas nimetame valijaks valimisnimekirjas olevat isikut. Serveriks nimetame häälte kogumiseks/lugemiseks kasutatavat masinat koos selles oleva tarkvaraga. Kliendiks nimetame suvaliselt osapoolt (sh ka valijat), mis ei ole server.

2.2.1 Valija/kliendi poolt sooritatavad ründed

Klient võib sooritada VISi vastu järgmiseid ründeid:

1. Mittevalija võib proovida hääletada/valija võib proovida hääletada teise legaalse valija nimel. Osaline lahendus: valija autentimine hääletamisel serveritarkvara poolt. Lisaprobleemid: kliendiarvuti peab olema turvaline (millegi autentimine peab olema võimatu, ilma et valija seda teaks). Autentsust on keeruline saavutada (ID-kaarti saab varastada). Server võib autentsust mitte kontrollida.

2. Valija võib hääletada ebakorrektselt (hääletada mitme kandidaadi poolt korraga, hääletada mitte-eksisteeriva kandidaadi poolt, saata serverile suvaline bitijada, ...). Lahendus: serveritarkvara peab kontrollima hääle kehtivust (vastavust spetsifikatsioonile). Lisaprobleemid: kliendiarvuti peab olema turvaline (häälte konstrueerimine peab olema võimatu, ilma et klient seda teaks). Server võib korrektsust mitte kontrollida.

3. Valija võib hääletada mitu korda. Osaline lahendus: serveritarkvara peab pidama arvet kõigi hääletajate üle, ning topelthääletamise puhul kas teist häält mitte arvestama, või esimese kehtetuks tunnistama. Lisaprobleemid: kliendiarvuti peab olema turvaline (häälte konstrueerimine peab olema võimatu, ilma et klient seda teaks). Server võib korrektsust mitte kontrollida.

4. Klient võib süüdistada serverit ebakorrektses häältelugemises, oma hääle arvestamata jätmises jne. Osaline lahendus: kõik e-valimiste süsteemi sammud peavad olema verifitseeritavad, ning süüdlased iga sammu rikkumises tuvastatavad (EVIS peab rahuldama *jälitatavuse* nõuet). Lisaprobleemid: kliendiarvuti peab olema turvaline (klient võib väita, et tema ei ole süüdi, kui häälte konstrueerimine ilma tema kaasabita on võimalik). Sama nõue kehtib serveriarvuti kohta.

5. Klient võib ummistada serveri võrguliiklust korduva ülehääletusega. Osaline lahendus: kasutada teenusetõkestamise rünnete (*Denial of Service attacks*) vastaseid meetmeid. Lisaprobleemid: sellised meetmed ei ole täielikud.

6. Klient võib katkestada füüsiliselt mõne serveri võrguühenduse. Osaline lahendus: kasutada duplitseeritud servereid. Lisaprobleemid: duplitseerida ei saa lõpmatult.

7. Klient võib katkestada füüsiliselt mõne valija võrguühenduse. Lahendus: lubada valida näiteks mobiilsidet kasutades, säilitada tavaliste valimiste võimalus. Lisaprobleemid: mobiilside pole turvaline. Kas valijad on motiveeritud valimisjaoskonna külastamisest pärast “tehnilisi vigu”?

8. Klient võib sundida (või meelitada) valijat hääletama endale sobiva kandidaadi poolt. Osaline lahendus: kasutaja ei saa tõestada, et ta hääletas just selle kandidaadi poolt. Lubada valijatel mitu korda hääletada (arvesse läheb viimane hääletus). Lisaprobleemid: Ümberhääletustest ei tohi “sundijaid” teavitada.

9. Üritada teada saada teiste valijate hääli. Osaline lahendus: hääletamine peab olema salajane. Lisaprobleemid: igavesti kestvat salajasust ei saa garanteerida. Kliendiarvuti peab olema turvaline (arvuti ei tohi kõrvalkanalitesse saata paare (valija, tema hääl)). Serveriarvuti peab olema turvaline.

10. Üritada segada häälte korrektset kogumist/lugemist. Osaline lahendus: nii häälte kogumine kui ka häälte lugemine peavad toimuma turvalistes masinates.

2.2.2 Serveri ründed EVISi vastu

Pahatahtlik server võib sooritada kõiki neid samu ründeid, mida suvaline mittevalijast klientki. Lisaks sellele

1. Server võib jätta valijate hääli arvestamata. Osaline lahendus: valijad peavad saama kontrollida, et nende hääled on arvestatud. Serverite tegevus peab olema duplitseeritud. Lisaprobleemid: Kliendid peavad kontrollimist teostama turvalisest masinast. Internetiühendus võib katkeda. Kuidas garanteerida, et vaid üksikud serverid “petavad”?

2. Server võib häältelugemisprotsessi mõnel muul viisil valesti toime panna. Osaline lahendus: nii valijad kui vaatlejad peavad saama kontrollida häältelugemise korrektsust. Serverite tegevus peab olema duplitseeritud. Lisaprobleemid: Kliendid peavad kontrollimist teostama turvalisest masinast. Internetiühendus võib katkeda. Kuidas garanteerida, et vaid üksikud serverid “petavad”?

3. Server võib häältelugemise protsessis mitte osaleda kas vääramatu jõu või pahatahtlikkuse tagajärjel. Osaline lahendus: serverite tegevus peab olema duplitseeritud. Lisaprobleemid: Kuidas garanteerida, et vääramatu jõud mõjub vaid üksikutele serveritele?

4. Server võib üritada teada saada individuaalsete valijate hääli. Osaline lahendus: hääletamine peab olema salajane, nii et ka pahatahtlik server tohib ainult teada saada iga kandidaadi poolt antud häälte koguarvu, mitte aga individuaalsete valijate poolt antud hääli. Lisaprobleemid: igavesti kestvat salajasust ei saa garanteerida. Kliendiarvuti peab olema turvaline (arvuti ei tohi kõrvalkanalitesse saata paare (valija, tema hääl)). Serveriarvuti peab olema turvaline ja duplitseeritud.

2.3 Eeldused e-valimiste korraldamise jaoks

Rünnete klassifikatsioonist võime teha järgmised järeldused, mida võib ka pidada eeldusteks e-valimiste turvalise korraldamise jaoks. Me ei too alljärgnevalt kaugeltki kõiki eeldusi; ülevaade [Ins01] on siinkohas oluliselt täielikum. (Samas on mainitud ülevaatest puudu osad meie poolt identifitseeritud probleemid.)

2.3.1 Krüptograafiline protokoll

E-valimiste ajal kasutatav krüptograafiline protokoll peab olema konstrueeritud nii, et

1. Iga hääl on autenditud (häält saadab digitaalallkiri). Server peab häälte autentsust kontrollima.

2. Hääli saadavad hääle korrektsuse tõestused. Server peab häälte korrektsust kontrollima.

3. E-valimised peavad rahuldama häälte salajasuse nõuet: server (ega keegi teine) ei tohi teada saada, kelle poolt valijad hääletasid.

4. Korrektsus: server peab teada saama häälte “summa”, ehk seda, kui mitu hääletajat summaarselt hääletas iga kandidaadi poolt.

5. Protokoll peab töötama ka siis, kui “vähemus” serveritest on ebaturvalised.

6. Protokoll peab olema universaalselt verifitseeritav. Kõigil soovijatel peab olema võimalik verifitseerida, et serveri poolt arvutatud "summa" vastab antud häältele. Sealjuures peab iga valija saama kontrollida, et tema häält arvestati lõpptulemuse arvutamisel.

7. (Ideaalis:) valikuvabadus. Protokoll peab valijal võimaldama valida nii, et ta ei saaks häälte ostjale või sundijale tõestada, kelle poolt ta hääletas. Võimaluse korral peaks hääl sisaldama varjatud "vihjet" serverile, et seda häält on ostetud ning seda häält ei loetaks või loetaks "tagurpidi". Juhul kui valija käib ümberhääletamas, ei tohi sundija saada seda verifitseerida.

Enamus ülaltoodud nõudeid on tänapäevaste krüptograafiliste protokollide abil lahendatavad [CGS97, HS00, Mür00]. Lisaprobleemiks, mida tuleb kindlasti märkida, on anonüümsuse "kadu", kui serverite võtmed avalikuks tulevad, või anonüümsuse kaitseks kasutatav krüptosüsteem lahti murtakse.

Analoogiline probleem tekkis ja lahendati (muu hulgas digitaalallkirja seaduse jaoks vajaliku) ajatembelduse probleemi käsitledes [BHS92, BLLV98]. Nimelt, kui digitaalallkirja tahetakse uuendada, võib sama teate uut salajast võtit või krüptograafilist signatuuriskeemi kasutades ülesigneerida. Samas on anonüümsuse kadu jääv: pärast serveri(te) võtme(te) avalikuks tulemist (või vastava krüptosüsteemi lahtimurdmist) jääb avalikuks tulnud hääl endiselt avalikuks. Vahe on selles, et signeeritav dokument ei ole enamasti salajane, samas kui hääl seda on.

Ka antud probleemile ei ole meie teada olemas efektiivset lahendust (kuigi Crameri, Gennaro ja Schoenmakersi artikkel [CGS97] tõstatab selle teema vajalikkust, ei paku nad välja ühtegi tõeliselt praktilist lahendit.), ning see väärib tõsist uurimistööd. Ei ole välistatud, et 15 aasta pärast ei toimu sõjaväelist riigipööret, mille jooksul hukatakse kõik, kes 15 aasta jooksul on mingi valitud erakonna poolt hääletanud. Seega, *valijate anonüümsus peab olema jääv.*

Ebatäiuslikuks lahendiks on serverite võtmete hoidmine turvalises riistvaras, ning väga konservatiivse krüptograafia kasutamine (näiteks 8192-bitised RSA võtmed). Samas konservatiivne krüptograafia on aeglane, eriti mobiilseadmetes (telefonid ja PDA-d), ning seega piirab e-valimiste kasutajate ringi. Samuti suurendab see oluliselt serverite töömahtu (8192-bitine RSA krüptimine on ligikaudu 500 korda aeglasem kui 1024-bitine RSA krüptimine!). Veel üheks võimaluseks on häälte kustutamine serveritest võimalikult vara, kuid seda peaksid tegema *kõik serverid ning verifitseerijad/vaatlejad*, mida aga ei saa tingimata eeldada. Ka siinkohas on olemas täiesti ootamatuid probleeme. Nii näiteks saab lugeda kõvakettalt kustutatud andmeid, kasutades suhteliselt lihtsalt tehnoloogiat:

kõvaketas on füüsiline objekt, mis nö “deformeerub”, kui temale midagi salvestatakse.

Rõhutame, et enamus toodud nõuetest on tänapäevaste krüptograafiliste meetodite abil lahendatavad. Peatükk 3 toob ühe lihtsama näite, mis seda ka demonstreerib.

Suundi edasiseks uurimistööks

Käesolev paragrahv võtab lühidalt kokku vajaliku edasise uurimistöö suunad.

Vihje andmine ning ümberhääletamise verifitseerimatus on peatükis 2.3.1 toodud nimekirjas ainuke originaalne nõue, mida me pole enne kohanud. Seetõttu ei ole teada ka lahendusi. Ümberhääletamise verifitseerimatus näib olevat vastuolus universaalse verifitseeritavusega. Ehk: kui me tahame saavutada sundimatust, siis väga tõenäoliselt peame ohverdama verifitseeritavuse. Samas rõhutame, et viimast küsimust pole uuritud.

Nii mõlema eelmainitud küsimuse kui ka informatsiooniteoreetiliselt turvaliste e-valimiste uurimiseks on vajalik algatada uurimisprogramm, et lahendada järgmised probleemid:

1. Välja töötada sundimatu e-valimiste skeem või näidata, et sellist pole olemas. (Näiteks ei ole sellist süsteemi olemas, kui inimene saab oma salajast võtit maha müüa.)

2. Välja töötada e-valimiste skeem, kus valijad püsivad anonüümsed ka siis, kui serverite võtmed avalikuks tulevad ning krüptosüsteem murdub. Üheks võimalikuks lahendiks on uurida, kas on võimalik saavutada *informatsiooniteoreetilist anonüümsust*: sellist anonüümsust, mis ei sõltuks teatud eelduste (tüüpi “1024-bitine RSA on tugev”) kehtimisest.

3. Uurida “konservatiivseid krüptosüsteeme”, mis sama turvalisuse astme juures oleksid oluliselt kiiremad kui (näiteks) 8192-bitine RSA.

2.3.2 Kliendi arvuti

Kliendi arvuti on piisavalt turvaline. St:

1. Arvuti ei ole võimeline andma digitaalallkirju bitijadadele, millele allkirja andmiseks kasutaja pole arvutit volitanud. Sealjuures peab olema valija kindel, et digiallkiri anti justnimelt tema valitud häälele. Lahendus: di-

giallkiri antakse füüsiliselt turvalises seadmes, mille tarkvara ei saa keegi ilma kasutaja teadmata modifitseerida. Seade peab olema võimeline nii signeerima kui ka tegeliku hääle ja signeeritava bitijada vahelist vastavust kontrollima. Seade peab olema "varastamiskindel" (nõudma kasutajalt enne hääletamist piisavalt turvalise parooli sisestamist).

2. Arvuti turvalisus on oluline nii selleks, et kolmandad osapooled (näiteks viiruse kirjutajad) ei saaks valija häält modifitseerida, kui ka selleks, et valija ei saaks hiljem oma arvutit süüdistades häält tagasi võtta.

3. Kuigi seda ei nimetatud kordagi eelnevalt, peab klienditarkvara olema *lihtsalt mõistetav* ning *üheselt mõistetav*. Klient peab olema suuteline valima üheselt oma kandidaadi poolt (see ei ole triviaalne, tuletagem meelde 2000. aasta USA presidendi valimisi Floridas, kus paljud valijad kaebasid valimissedelite keerukuse üle!). Välistatud peab olema hääle "kogemata" andmine. Kõikvõimalike turvakontrollide (kas server arvestas mu häälega?) tegemine peab olema lihtne ja intuitiivne.

Personaalarvutil ei hakka sellist turvalisustaset ilmselt niipea olema, ning spetsiaalse riistvara muretsemine valimisteks on ilmselgelt liiga kallis. Alternatiivseks lahendiks on mobiiltelefonide kasutamine. Mobiiltelefonide heaks omaduseks on see, et kasutaja (ega keegi teine) ei saa neil olevat programmtarkvara hõlpsasti modifitseerida. Samas on halbadeks omadusteks väike ekraan (mis muudab valimiste kasutajaliidese arusaamatult segaseks), tõenäosus saada varastatud, väike arvutusvõimsus ning GSM-võrgu praktiliselt täielik ebaturvalisus. Osaliseks lahenduseks võib olla Sonera Smarttrusti taoline kiipkardi lahendus (mis ei pruugi olla odav!), mis sisaldab signeerimis- ja krüptimisvõtmeid, ning mis on võimeline hääli genereerima piisavalt kiiresti.

Märgime, et antud temaatikat (turvalise arvuti olemasolu) on ka Eestis kergelt uuritud digitaalallkirja seaduse kontekstis [FHW00].

2.3.3 Serveri arvuti

Serveri arvuti on piisavalt turvaline. St serveri arvuti jälgib eeltoodud krüptograafilist protokolli ja ei tee mitte midagi muud.

1. Serveri arvuti turvalisust on kergem saavutada, kui valija arvuti turvalisust, kuna nende turvalisuse kontrolliks võib valitsus vms organ eraldada piisava summa raha.

2. Garanteerimaks, et valimised toimuksid ka vääramatu jõu korral, peab serveri tegevus olema duplitseeritud. Serverid peavad asuma füüsiliselt eraldatud, füüsilise järelvalve all olevates kohtades, ning kasutama ideaalis erinevate Interneti teenusepakkujate teenuseid.

3. Kõigil erakondadel peab olema võimalus teostada serverite turvaaudit. Igal piisavalt suurel erakonnal (või erakondade ühendusel) ja erapooletul organisatsioonil (näiteks Eesti Teadlaste Liidul, Eesti Infotehnoloogia Seltsil, Eesti Kaubandus-Tööstuskojal, Eesti Teaduste Akadeemial, ...) võiks olla õigus, pärast ametlikku eelregistreerimist panna üles üks sõltumatu server. Garanteerimaks, et üksikute ebaturvaliste serverite olemasolul terve süsteem ei lakkaks funktsioneerimaks, tuleb e-valimised üles ehitada läviusalduse põhimõtet rakendades. Intuitiivselt, kui vähemalt 2/3 serveritest on usaldusväärsed ja töökindlad, siis saab arvestada "enamuse" tahtega. (Krüptograafias on läviusalduse mõiste keerulisemalt defineeritud, vt peatükki 3.) Lisaprobleemid: on ebaselge, kas Eestis leidub piisavalt palju *konkureerivaid* erakondi ja *sõltumatuid* erakondi, kes oleksid rahaliselt ja inimpotentsiaalilt võimelised tegema sõltumatut turvaauditit.

4. Serverite salajased võtmed peavad paiknema ülimalt turvalises riistvaras. Viimane on vajalik võtmelekkimise vältimiseks.

5. Serverid peavad säilitama hääli kuni häältelugemise lõpuni, et võimaldada häälte ülelugemist. Potentsiaalselt peaksid serverid hääli salvestama piisavalt kaua, et võimaldada lahendada kõikvõimalikke kerkivaid kohtuprobleeme.

6. Arvuti turvalisus on oluline nii selleks, et kolmandad osapooled (näiteks viiruse kirjutajad) ei saaks valijate häält modifitseerida, kui ka selleks, et valija ei saaks hiljem *serverit* süüdistades häält tagasi võtta, väites, et tema digitaalallkiri häälel on sinna sattunud tema tahtest sõltumatult.

Lühike soovitus: soovitame silmas pidada turvaliste arvutite loomise initsitatiivi *Trusted PC* [Tru].

2.3.4 Võrguühendus

Võrguühendus on piisavalt turvaline. St:

1. Nii kliendiarvutid, serverid kui ka *kõik nendevahelised marsruuterid ja teised arvutid* peavad olema kõrgendatud turvalisusega teenusetõkestamise rünnete vastu. Lisaprobleemid: siinkohas saab turvataset vaid kõrgendada, kuid mitte absoluudini viia. Hajusrünnete vastu, mida sooritavad tuhanded üle Interneti paiknevad arvutid, on praktiliselt võimatu e-valimissüsteeme kaitsta.

Kuna me ei ole antud ala spetsialistid, piirdume me siinkohal ainult toodud üldsõnalise soovitusega. Edasiseks lugemiseks soovitame näiteks ülevaadet [Ero00].

2.3.5 Administratiivsed meetodid

Administratiivsed, valimisseaduslikud lahendused.

1. Vältimaks valijate häälte ostmist ja valijate sundimist, aga samas ka vääramatuid jõude (võrguühenduse puudumist), peab valijatel olema võimalus peale e-valimiste lõppu minna ja uuesti valida.

2. Nagu öeldud, peab valimiste keskserver olema duplitseeritud. Samas ei pruugi (finantskaalutlustel) serverit olla igas maakonnas. Seega kaob vajadus valimisjaoskondade järele, kuid kasvab vajadus kõrgendatud turvaastmega keskvalimisjaoskonna järgi. E-valimiste jaoks on mõistlik vaid ühte jaoskonda töös hoida ka tänu kvalifitseeritud inimeste nappusele (vt järgmist eeldust).

3. Ebaselgeks muutub valimiskomisjoni funktsioon, ja nende usaldatavuse alammäär. Kui traditsiooniliste valimiste ajal on valimiskomisjon vastutav kõikide vastavas jaoskonnas toimuvate valimiseeskirjade rikkumiste eest, siis e-valimiste korral valimiskomisjonile sellist vastutust anda ei saa. Valimiskomisjoni liikmed ei saagi olla piisavalt kompetentsed arvutite turvaliseks muutmisel; Eesti Vabariigis on vastava kompetentsitasemega inimesi alla viie (kui üldse). Kõikide vigade eest ei saa ka kompetentseid inimesi süüdistada. Näide: mõned aastad tagasi avastati viga Pentium protsessoris, mille tõttu teatud tüüpi teaduslikud arvutused andsid valesid vastuseid.

4. Tänu eelmisele punktidele tuleb lisatähelepanu pöörata selliste inimeste koolitamisele, kes oleks kompetentsed andmeturbes, ning tuleksid toime

arvuti riist- ja tarkvara sertifitseerimisega, krüptograafiliste protokollide koostamise ja verifitseerimisega.

5. Tuleb tegeleda ka tavaliste inimeste arvuti- ning andmeturbealase koolitamisega. Küsides retooriliselt: mis kasu on turvalisest e-valimissüsteemist, kui inimesed kasutavad seda valesti, näiteks ei kontrolli digitaalallkirja e-valimiste tarkvaral?

Peatükk 3

Realiseerimise alternatiivid

3.1 E-valimise realiseerimise erinevad võimalused

E-valimisi saab realiseerida ühe serveri poolt pakutava teenusena. Eeldab seda, et kõik süsteemi kasutajad usaldaksid seda serverit, sealhulgas selle operaatoreid. Siin ei tulene täieliku usalduse vajadus mitte sellest, et üks server võiks talle saadetud hääli maha kustutada (sellist käitumist saab vältida näiteks sõltumatu ajatempliserveri kasutamisel, mis registreeriks kõik saadetud hääled). Ühe serveri puhul on võimatu garanteerida, et server aktsepteerib temale suunatud hääli. Server võib nii pahatahtlikult filtreerida teatuid võrguaadresse, aga samuti võib tema võrgukoormus olla liiga suur, mille tagajärjel server pole võimeline kõiki hääli aktsepteerima. Ei ole võimalik kindlaks teha, kumb juhtudest tegelikkuses aset leidis.

Samuti on tänapäevaks pakutud efektiivsete ja krüptograafiliselt turvaliste e-valimissüsteemide puhul hääled krüptitud serveri avaliku võtmega. Ühe serveri puhul ei saa garanteerida, et server ei dekrüpti lahti kõiki hääli eraldi. (Märgime, et on olemas erinevaid ühe serveriga lahendusi, mida me käesolevas materjalis ei kirjelda. Neist parimaid lahendusi ei tuleks alahinnata.)

Teise, ja parema võimalusena, saab e-valimisi realiseerida N serveri poolt pakutava teenusena, kusjuures teenus töötab seni, kuni N serverist ülimalt T (kus teoreetilistel põhjustel $T < N/2$) toimivad ebakorrektselt (*läveusaldus*). Selline usalduse jagamine eeldab, et erinevaid servereid kontrollivad erinevad osapooled -näiteks konkureerivad poliitilised jõud, apoliitilised asutused, akadeemilised organisatsioonid ja välisvaatlejad.

3.2 Mitme serveriga lahendus

Järgnevalt kirjeldame mitme serveriga lahendust *tehniliselt*. Tehnilisele lahendusele peab kaasnema ka *organisatoorne* lahendus. Nii näiteks peab töötama turvaline mehhanism hääletajate ning serverite avalike võtmete levitamiseks. Viimaseks võib olla kas PKI ehk avaliku võtme infrastruktuur, või mõni lihtsam lahendus, näiteks registris hoitav vastavus hääletajate ning nende avalike võtmete nimekirja vahel; serverite avalikke võtmeid saab levitada näiteks valitsuse vastava ametniku poolt tavameetodil allkirjastatult. Neid mehhanisme me ei kirjelda.

Seega, järgnevalt eeldame, et igal e-valimistel osaleval hääletajal on olemas digitaalallkiri, millele vastav avalik (verifitseerimis-) võti on serveritele ja kõigile vaatlejatele autentsel teel kättesaadav. Eeldame samuti, et valijate ja serverite arvutid on turvalised ning ka võrguühendus on olemas. Kõik serverid *jagavad* ühte avaliku ja salajase võtme paari, nii et erinevatel serveritel on erinevad salajased võtmed kuid ühine avalik võti. Eeldame, et serverite avalik võti on autentsel teel kättesaadaval kõigile hääletajatele ning vaatlejatele. Serverite võtmetele püstitatavaid nõudeid käsitleme lähemalt järgmises lõigus.

3.2.1 E-valimiste ettevalmistamine

Järgnevalt kirjeldame lühidalt Crameri, Gennaro ja Schoenmakersi e-valimiste skeemi [CGS97]. Kuigi tegemist on ühe tuntuima ning ka parima skeemiga, tasub meeles pidada ka alternatiivsete skeemide olemasolu, kuna mõned neist (nagu näiteks hiljuti publitseeritud [DJ01]) on efektiivsemad või turvalisemad.

Olgu N serverite koguarv ning $T > N/2$ usalduslävi. (Reaalsetel valimistel näiteks $N = 7$ ning $T = 4$.) Serverite avalikud võtmed ning salajane võti peavad rahuldama järgnevaid tingimusi:

1. Krüptitud teate saatmiseks kõigile N serverile peab hääletaja teate krüptima vaid üks kord, kasutades serverite ühist avalikku võtit.

2. Jagagu teatud alamhulk N serverist sama krüptitud teadet (mis võib aga ei pruugi olla mingi hääletaja hääl). Viies läbi nn *lävedekrüptimise* protseduuri, kus iga server kasutab oma salajast võtit, saab serverite alamhulk teada originaalteate, kui vähemalt T neist on ausad.

3. Kui alamhulgas pole vähemalt T ausat serverit, siis dekrüptimine ebaõnnestub.

Lävekrüptimine on seega kasutaja jaoks läbipaistmatu; hääletaja (täpsemalt hääletaja arvutis olev tarkvara) peab vaid oma hääle edastama vähemalt T (eelistatavalt kõigile N) serverile.

Serverid peavad enne valimiste alguses täitma ühise lävevõtmegenereerimise algoritmi, mille tagajärjel tekib N salajast võtit ning 1 avalik võti. Viimane levitatakse autentselt kõigile hääletajatele ning vaatlejatele. Edaspidises tähistame serverite avaliku võtmega krüptitud teadet M kui $E(\mathsf{server}, M)$. Krüptitud teatele C vastavat serverite poolt ühiselt dekrüptitud teadet tähistame kui $D(\mathsf{server}, C)$. Muidugi peab kehtima võrdus $D(\mathsf{server}, E(\mathsf{server}, M)) = M$.

Lävekrüptimist/dekrüptimist on võimalik efektiivselt teostada enamus tuntud krüptosüsteemide korral, k.a. neist enimtuntuima, RSA, korral. Siiski on RSA puhul efektiivsus tunduvalt väiksem kui mõnede teiste süsteemide (näiteks elliptilistel kõveratel põhinevate krüptosüsteemide korral). Samas, nagu järgnevalt näeme, krüptosüsteemile esitatavad muud nõudmised *välistavad tihti RSA*, mistõttu võib vajalikuks osutuda alternatiivsete krüptosüsteemide kasutamine. Igal juhul ei saa hääle krüptimiseks kasutada sama võtit, mida kasutatakse signeerimiseks.

3.2.2 Valimised

Tüüpilises e-valimiste süsteemis peab iga hääletaja tegema järgmised sammud. Pärast protseduuri üldist kirjeldamist selgitame me lühidalt tehnilisi üksikasju. (Järgnevas tähistame konkreetset hääletajat suure A-ga, samuti on temale vastavad muutujad (tema hääl, salajane ja avalik võti jne) on indekseeritud A-ga.)

1. Hääletaja A otsustab ühe kandidaadi kasuks ning hääletab, sisestades arvutisse mingid andmed (vajutades hiirenuppu mingil ekraanipiirkonnal, sisestades kandidaadi nime/numbri käsitsi vms).

2. Arvutis teisaldatakse sisestatud hääl valija A eeliskandidaadile vastavaks numbriks v_A. (Seos kandidaatide ja neile vastavate numbrite vahel peab olema avalik ja efektiivselt verifitseeritav.) NB! Kõik järgnevad sammud toimuvad vaikimisi arvutis, kui hääletaja pole otsustanud neid turvalisuse kaalutlustel käsitsi läbi viia. Lihtsuse mõttes tähistame tegevuste sooritajat endiselt tähega A.

3. A krüptib hääle v_A, kasutades serverite ühist avalikku võtit. Olgu tulemuseks krüptogramm $c_A = E(\mathsf{server}, v_A)$.

4. A signeerib väärtuse c_A, kasutades oma signeerimisvõtit. Olgu tulemuseks digitaalsignatuur $d_A = S(A, c_A)$.

5. A genereerib lühikese *hääle kehtivuse tõestuse* P_A.

6. A edastab kolmiku (c_A, d_A, P_A) teadetetahvlile, kus kolmik arhiveeritakse, vastavalt eelnevalt toodud teadetetahvli kirjeldusele. Hääletajale tagastatakse sertifikaat kolmiku vastuvõtmise kohta. Teadetetahvel peab rahuldama vähemalt järgmisi tingimusi:

   (a) Hääletaja saab kontrollida, et tema hääl on tahvlil kirjas. Juhul kui ei ole, võib hääletaja protestida.

   (b) Serverid ning vaatlejad (sh teised hääletajad) saavad kontrollida signatuuri ja hääle kehtivuse tõestuse õigsust.

   (c) (Optsionaalselt:) Hääletajad peavad saama oma hääli tahvlilt kustutada ja/või uutega asendada. (Nagu mainitud, ei sobi see hästi kokku teadetetahvli tavalise definitsiooniga.)

Serverid teevad järgnevat:

1. Server loeb teadetetahvlilt (c_A, d_A, P_A).

2. Juhul kui d_A pole A signatuur krüptogrammil c_A või P_A pole korrektne hääle kehtivuse tõestus, ei tee server midagi. (Server võib logida vastava teate, kui see ei ava akent DoS rünnetele.)

3. Saabunud kolmik (c_A, d_A, P_A) avaldatakse teadetahvlil, hääletajaga A vastavusse seatud lahtrisse.

3.2.3 Häälte kokkulugemine

Serverid teevad järgmist:

1. Kõigile hääletustahvlil olevatele väärtustele c_i (oletame, et neid on n tükki) rakendadakse spetsiaalset funktsiooni Sum, nii et $\mathsf{Sum}(c_1, \ldots, c_n)$ annab tagasi listi $(d_1, \ldots, d_m)$, kus $d_j = E(\mathsf{server}, s_j)$ ning s_j on j-nda kandidaadi poolt antud häälte koguarv. Antud funktsioon Sum on arvutatav kõigi osapoolte (mitte ainult serverite) poolt. Muuhulgas saavad vaatlejad verifitseerida, et serverid on väärtuse Sum korrektselt arvutanud (sh mitte välja jätnud ühtegi legaalset häält).

2. Serverid dekrüptivad ühiselt, kasutades lävidekrüptimist, suurused d_j. Saadud tulemused s_j koos tõestustega Q_j, et $s_j = D(\mathsf{server}, d_j)$ (st, et dekrüptimine oli korrektne), postitatakse teadetahvlil kõigi poolt verifitseerimiseks.

3. Vaatlejad võivad teatud, eelnevalt spetsifitseeritud pikkusega, perioodi jooksul verifitseerida, et nii suurused d_j kui ka suurused s_j on korrektselt arvutatud. (Esimeste verifitseerimiseks kasutatakse kõigi poolt arvutatavat funktsiooni Sum, viimaste verifitseerimiseks aga suurusi Q_j.)

4. Pärast verifitseerimiste lõppu kuulutatakse tulemused s_j ametlikeks. Edasine (kuidas kellelegi antud häälte arv mõjutab valimiste lõpptulemusi) sõltub juba valimiste enda tüüpist.

3.2.4 Krüptograafilised nüansid

Tänu lävekrüptograafia kasutamisele peame eeldama, et vähemalt pooled serveritest on usaldusväärsed. Vastasel korral võiks pettev enamus dekrüptida suvalise väärtuse c_i ja saada nii teada valija i hääle.

Eelnevalt postuleerisime teatud funktsioonide (nagu näiteks Sum) olemasolu. Samuti nõudsime, et leiduksid tõestused (näiteks) selle kohta, et teatud väärtus on saadud teise väärtuse dekrüptimisel. Sellised funktsioonid ja tõestused on tõepoolest olemas, kuid mitte kõigi krüptosüsteemide puhul; samuti on nad osade krüptosüsteemide puhul oluliselt efektiivsemad kui teiste puhul. Ilma liigselt matemaatikasse laskumata toome järgnevas vaid ühe (lihtsa) näite selle kohta, kuidas saab funktsiooni Sum arvutada. Järgneva juures on oluline tähele panna, et isegi kahe kandidaadi korral ei lange serverite tegevus 100% ühte eelnevas toodud definitsiooniga (kuigi lõpptulemus on korrektne!).

Olgu valimistel kasutataval krüptosüsteemil järgmine, *homomorfsuse*, omadus: iga M ja N korral, $E(\mathsf{server}, M) \cdot E(\mathsf{server}, N) = E(\mathsf{server}, M+N)$.

Kui krüptosüsteem rahuldab homomorfsuse omadust, ning valimistel on vaid kaks kandidaati, kelle poolt hääletamiseks krüptitakse vastavalt kas suurus -1 (esimene kandidaat) või 1 (teine kandidaat), siis saab funktsiooni Sum arvutada järgmiselt:

$$X = \mathsf{Sum}(d_1, \ldots, d_m) = E(\mathsf{server}, d_1) \cdot \cdots \cdot E(\mathsf{server}, d_m) \quad .$$

Tõepoolest, sellisel juhul on $d = d_1 + \cdots + d_m$ võrdne erinevustega teise kandidaadi poolt antud häälte arvu ja esimese kandidaadi poolt antud häälte

arvu vahel. Lähtudes homomorfsuse omadusest on $X = E(\mathsf{server}, d)$. Seega on $(m + D(\mathsf{server}, Y))/2 = (m + d)/2$ võrdne teise kandidaadi poolt antud häälte arvuga, ning $(m - D(\mathsf{server}, Y))/2 = (m - d)/2$ on võrdne esimese kandidaadi poolt antud häälte arvuga. Konkreetse näite varal, kui hääli kokku oli $m = 100$ ning $d = 80$, siis hääletas esimese kandidaadi poolt $(100 - 80)/2 = 10$ ning teise kandidaadi poolt $(100 + 80)/2 = 90$ valijat.

Antud juhul on hääle korrektsuse tõestuseks P_A bitistring, mille verifitseerimise järel aktsepteerib verifitseerija vaid siis, kui $c_A = E(\mathsf{server}, -1)$ või $c_A = E(\mathsf{server}, 1)$. Tõestus peab olema selline, et aktsepteerimine toimuks ilma, et verifitseerija saaks teada, millise juhuga (kas $c_A = E(\mathsf{server}, -1)$ või $c_A = E(\mathsf{server}, 1)$) konkreetselt tegu on. Selliseid tunnistusi on võimalik konstrueerida efektiivselt peaaegu kõigi turvaliste krüptosüsteemide jaoks.

Samas homomorfsuse omadust ei rahulda mitte iga krüptosüsteem; näiteks ei ole RSA homomorfne. Samuti on toodud skeemi üldistus valimistele, kus kandidaatide arv on oluliselt suurem kui 2, ebatriviaalne, ehkki võimalik. Esimesed *efektiivsed* skeemid paljukandidaadiliste e-valimiste jaoks on välja pakutud alles sellel aastal. Lõpuks toome ühe konkreetse näite krüptosüsteemist, mis on homomorfne ning mida saab kasutada lävikrüptimiseks.

ElGamali krüptosüsteemis valitakse esmalt suur algarv p, kõik järgnevad tehted toimuvad modulo p. Seejärel valitakse teatuid lisatingivusi rahuldav arv g, mis on väiksem kui p. (p, g) on süsteemi parameetrid. Kasutaja A salajaseks võtmeks on arv x ning avalikuks võtmeks arv $h = g^x \mod p$. Avateksti M krüptimisel kasutaja A avaliku võtmega genereerib kasutaja B esmalt juhuslikult arvu R; saadavaks krüptogrammiks on $E(A, M) = (g^M h^R \mod p, g^R \mod p)$. ElGamali krüptosüsteem on homomorfne, kuna $E(A, M) \cdot E(A, N) = (g^M h^R, g^R) \cdot (g^N h^Q, g^Q) = (g^{M+N} h^{M+N}, g^{M+N} = E(A, M + N)$, (Viimane võrdus tuleneb sellest, et kui R ja Q on juhuslikud arvud, on seda ka $R + Q$.)

Toodud e-valimiste skeemi kirjeldati esmakordselt Ronald Crameri, Rosario Gennaro ja Berry Schoenmakersi poolt artiklis [CGS97], kus on toodud ka lävekrüptimiseks vajalikud protseduurid. Toodud süsteemi on hiljem täiustatud Martin Hirti ja Kazue Sako poolt [HS00], kes lisasid süsteemile osad sundimatuse tagamiseks vajalikud omamised, ning Ivan Damgårdi ja Mads Juriku poolt [DJ01], kes optimiseerisid süsteemi juhu jaoks, kus kandidaatide arv on suurem kui kaks. Vähemtehnilise ülevaate (koos omapoolsete täiendustega) võib leida Oleg Mürgi semestritööst [Mür00], kust võib leida ka viiteid täiendavale kirjandusele. Sama skeemi implementatsiooni kirjeldab Veera Lehtoneni magistritöö [Leh00].

Kirjeldatud hääle korrektsuse tõestuse meetodit kirjeldati esmalt artiklis [CDS94]. Homomorfsetest krüptosüsteemidest on hetkel ilmselt tuntuim Pail-

lier'i krüptosüsteem [Pai99]. Digitaalsignatuuride ja muude krüptograafiliste objektide parimaks kirjelduseks on hetkel juba vananenud käsiraamat [MOV96].

Peatükk 4

Soovitused

Alljärgnevas toome mõned üldised soovitused e-valimiste tuleviku suhtes. Antud raport valmis väga lühikese aja jooksul (u. 20 inimpäeva), samas peaks järgmises punktis toodud iga alamlõigu uurimiseks kulutama vähemalt kolm inimaastat (õnneks ei pea seda kõike tegema Eestis; samu asju uuritakse ka rahvusvaheliselt).

1. Alustada teoreerilise/krüptograafilise uurimisprogrammiga. Nagu rõhutatud eelnevas, on e-valimiste tänapäevastes süsteemides mitmeid teoreetilisi puudusi, mida tuleks lahendada. Eeskätt tuleb mainida sundimatuse ning informatsiooniteoreetilise anonüümsuse tagamise uurimist.

2. Alustada sotsioloogilise uurimisprogrammiga. On selge, et lihtsad lahendused (veebipõhised, nagu e-pangandus) e-valimiste jaoks ei sobi. Millised vahendid on e-valimiste sooritamiseks rahva jaoks vastuvõetavad, nii rahaliselt kui ka psühholoogiliselt? Kuidas mõjutab e-valimiste toimumine üldiselt valijate suhtumist valimistesse?

3. Alustada praktilis-tehnilise uurimisprogrammiga. Milliseid samme on võimalik astuda, et tõsta koduarvutite üldist turvataset? Kas spetsiaalsetel e-valimisseadmetel oleks ka muid kasutusvaldkondi? Kas ja kuidas on võimalik kasutada mobiiltelefone valimiseks? Kuidas vältida teenusetõkestamisründeid? Kuidas konstrueerida lihtsaid, arusaadavaid kasutajaliideseid, nii et valimistel ei tekiks Florida-tüüpi arusaamatusi, kus valijad on kogemata valinud vale kandidaadi? Kuidas konstrueerida arusaadavaid ja turvalisi kasutajaliideseid puuetega valijate, kes on e-valimiste üks sihtgruppe, jaoks?

Ideaalis peaks eeltoodud uurimisprogrammid toimuma koostöös, sest krüptograafid ei tea tavaliselt palju sotsioloogiast, ja vastupidi.

Lisaks uurimisprogrammide alustamisele soovitame astuda järgmisi samme.

1. Osaleda rahvusvahelistes programmides. Hetkel on käimas Euroopa Ühenduse e-valimiste alane projekt "EU Cybervote", kes otsib asjast huvitatud osapooli. Esimene autor on antud projektiga väga vähesel määral juba seotud. On paratamatu, et Eestis ei ole niivõrd keerulise problemaatika käsitlemiseks piisavat inimressurssi, ning seega tuleb teha koostööd.

2. Koolitada inimesi. Inimesed ei saa aru ega taha aru saada enamustest andmeturbeprobleemidest, seetõttu on neid ka lihtne "petta" kõikvõimalikes e-kommertsrakendustes. Siiani ei ole pettusi eriti tihti toimunud just petturite motivatsioonipuuduse tõttu; samas e-valimiste tulemuste muutmisest võivad olla huvitatud konkureerivad erakonnad, välisriikide valitsused ning rahvusvaheline maffia. Et inimesed aru saaksid oma tegevuste tähtsusest, tuleb neile teadvustada andmeturbega seotud probleeme.

3. Toimida tasa ja targu. E-valimiste suhtes on hetkeks avalikkusele lubatud rohkem kui põhimõtteliselt võimalik on. Et mitte kompromiteerida e-valimiste ideed kui sellist, tuleks edaspidi tegeleda rohkem e-valimiste reaalse tagatausta ettevalmistamisega kui valdkonna ülepopulariseerimisega meedias.

Juhime tähelepanu sellele, et meie soovitused langevad põhiliselt kokku nende soovitustega (kuigi on lühemad ja seega mitte nii täielikud), mida valmistas ette USA presidendi korraldusel loodud komisjon ühe aasta jooksul [Ins01]. Analoogilisi soovitusi võib leida ka Avi Rubin'i artiklist [Rub00].

Peale ülaltoodud, ettevalmistavate, soovituste, riskime pakkuda ka järgmisi, praktilisemaid, soovitusi. Riskimise all mõtleme siin seda, et neid soovitusi esitades oleme *üli*optimistlikud, ning oleme valmis "taganema" neist soovitustest, kui eelmisi soovitusi täide ei viida.

- Viia (näiteks) ülejärgmiste Riigikogu valimiste ajal läbi referendum, milles on võimalik osaleda ka üle Interneti. Referendum on vaid üks valimiste erijuhte, kus ühe kandidaadi asemel eelistatakse ühte vastusevarianti. (Seega kõik andmeturbeprobleemid jäävad täpselt samaks.)

- Referendum *ei tohi* olla piisavalt oluline, et äratada üldist huvi selle nurjamise vastu. Samas *peab* olema võimalus referendumi tühistamiseks, kui

on tuvastatud ründeid e-referendumi vastu. Referendum *peab olema* piisavalt oluline, et motiveerida valijaid selles osalema, ning käituma nii, nagu oleks tegemist valimistega. Referendumil võib olla mitu erineva tähtsusega küsimust, milledest üks võiks olla e-valimiste toimumise vajadus.

- Referendumile peab saama vastata nii Interneti teel, kui ka valimisjaoskondades. E-referendum võiks toimuda *nädala* jooksul *enne* valimisjaoskondade avamist. (Pikk periood on vajalik teenusetõkestamise rünnete ja vääramatu jõu vastu võitlemiseks.) E-referendumil osalejatel *peab* olema ID-kaart, mille abil nad võivad registreeruda ka üle Interneti. Kõigil e-referendumil osalejatel *peab* olema võimalus oma häält tühistada valimisjaoskonnas.

- Täpsemad eeskirjad peab välja töötama valimisspetsialistidest, praktilise andmeturbe spetsialistidest ning krüptograafidest koosnev komisjon; eeldatav töömaht: vähemalt 1 inimaasta.

- Tarkvara peab olema valmis vähemalt kuus kuud enne e-referendumi algust, ja kättesaadav kõigile soovijatele tasuta, autentsel kujul (vt ka peatükki 2.1) enamlevinud platvormidele. Eeldatav töömaht tarkvara tegemiseks: vähemalt 1 inimaasta.

- Lähtudes saadud kogemustest ning täiendavast tööst vähemalt 2 inimaasta ulatuses otsustada e-valimiste korraldamise üle ülejärgmiste Riigikogu valimiste ajal (aastal 2007).

Lõpetuseks. Kuigi käesoleva raporti põhitoon on pessimistlik, on e-valimiste toimumine umbes 20 aasta pärast arvatavasti paratamatu. Ka Eesti Vabariik peab e-valimiste uurimise ja rakendamisega tegelema. *Meie pessimism on suunatud e-valimiste vastu aastal 2002, mitte aga e-valimiste kui protsessi vastu üldiselt*. Lähema kümne aasta jooksul on oodata Interneti (ja mobiilside) veelgi laialdasemat kasutuselevõttu kõigis elusfäärides. Paljud riistvaratootjad tegelevad juba praegu personaalsete turvakeskkondade loomisega, ning nende töö kannab loodetavasti vilja lähema viie aasta jooksul. Samuti on edusamme oodata krüptograafiliste e-valimisprotokollide juures. *Summa summarum*: soovitame valdkonnaga kursis olla ning seda edasi uurida.

Kirjandus

[BHS92] Dave Bayer, Stuart A. Haber, and WakefieldŠcott Stornetta. Improving the Efficiency And Reliability of Digital Time-stamping. In *Sequences'91: Methods in Communication, Security, and Computer Science*, pages 329–334. Springer-Verlag, 1992.

[BLLV98] Ahto Buldas, Peeter Laud, Helger Lipmaa, and Jan Villemson. Time-stamping with Binary Linking Schemes. In Hugo Krawczyk, editor, *Advances on Cryptology — CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 486–501, Santa Barbara, USA, August 1998. Springer-Verlag.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Yvo G. Desmedt, editor, *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer-Verlag, 21–25 August 1994.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In Walter Fumy, editor, *Advances on Cryptology — EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118, Konstanz, Germany, May 1997. Springer-Verlag.

[DJ01] Ivan Damgård and Mads Jurik. A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System. In Hideki Imai and Kil Hyun Nam, editors, *Public Key Cryptography '2001*, volume (to appear) of *Lecture Notes in Computer Science*, pages ??–??, Cheju Island, Korea, 13–15 February 2001. Springer-Verlag.

[Ero00] Pasi Eronen. Denial of service in public key protocols. In *Helsinki University of Technology Seminar on Network Security. Mobile Security '2000*, page 13, Sjökulla, 4–5 December 2000. Helsinki University of Technology, Department of Computer Science and Engineering, Telecommunications Software and Multimedia Laboratory. Available from `http://www.tml.hut.fi/Opinnot/Tik-110.501/`, as of March 2001.

[EVP92] Eesti Vabariigi põhiseadus, 28 June 1992. Kättesaadav aadressilt `http://seadus.ibs.ee/seadus/aktid/rh.s.19920628.1.19920703.html` (seisuga märts 2001).

[FHW00] Margus Freudenthal, Sven Heiberg, and Jan Willemson. Personal Security Environment on Palm PDA. In *Annual Computer Security Applications Conference*, page 23, Sheraton New Orleans, Louisiana, USA, 2000.

[HS00] Martin Hirt and Kazue Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Bart Preneel, editor, *Advances on Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 539–556, Bruges, Belgium, 14–18 May 2000. Springer-Verlag.

[Ins01] Internet Policy Institute. Report of the National Workshop on Internet Voting: Issues and Research Agenda, March 2001. Sponsored by National Science Foundation. Conducted in cooperation with the University of Maryland and hosted by the Freedom Forum. Available from `http://www.internetpolicy.org/research/results.html`, as of March 2001.

[Leh00] Veera Lehtonen. Implementation of a Robust Electronic Voting System, 2000.

[MOV96] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[Mür00] Oleg Mürk. Electronic Voting Schemes. Technical report, University of Tartu, Institute of Computer Science, 2000. Semester work. Available from

http://www.cs.ut.ee/~olegm/my_papers.english.html, as of March 2001.

[Pai99] Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Jacques Stern, editor, *Advances on Cryptology — EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238, Prague, Czech Republic, 2–6 May 1999. Springer-Verlag.

[Rub00] Avi Rubin. Security Considerations for Remote Electronic Voting over the Internet. *Sunworld*, October 2000. Available from http://avirubin.com/e-voting.security.html, as of March 2001.

[Tru] Trusted Computing Platform Alliance. Trusted PC Homepage. Available from http://www.trustedpc.org, as of March 2000.