



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

Aurimas Vengalis

**SAUGUMO GRĖSMĖS IR JŲ PREVENCIJA ELEKTRONINIO
BALSAVIMO SISTEMOSE
SECURITY THREATS AND THEIR PREVENTION IN ELECTRONIC
VOTING SYSTEMS**

Baigiamasis magistro darbas

Informacinių technologijų studijų programa, valstybinis kodas 621E14004

Duomenų gavybos technologijos specializacija

Informatikos inžinerijos studijų kryptis

Vilnius, 2017

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

TVIRTINU
Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

Aurimas Vengalis

**SAUGUMO GRĖSMĖS IR JŲ PREVENCIJA ELEKTRONINIO
BALSAVIMO SISTEMOSE
SECURITY THREATS AND THEIR PREVENTION IN ELECTRONIC
VOTING SYSTEMS**

Baigiamasis magistro darbas

Informacinių technologijų studijų programa, valstybinis kodas 621E14004

Duomenų gavybos technologijos specializacija

Informatikos inžinerijos studijų kryptis

Vadovas

(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

(Parašas)

(Data)

Lietuvių kalbos konsultantas

(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

(Parašas)

(Data)

Vilnius, 2017

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

Informatikos inžinerijos studijų kryptis

Informacinių technologijų studijų programa, valstybinis kodas 621E14004

Duomenų gavybos specializacija

TVIRTINU

Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

**BAIGIAMOJO MAGISTRO DARBO
UŽDUOTIS**

.....Nr.

Vilnius

Studentui (ei) Aurimas Vengalis

.....
(Vardas, pavardė)

Baigiamojo darbo tema: Saugumo grėsmės ir jų prevencija elektroninio balsavimo sistemose
patvirtinta 2016 m. gruodžio 20 d. dekanų potvarkiu Nr. 417fm

Baigiamojo darbo užbaigimo terminas 201 ____ m. _____ d.

BAIGIAMOJO DARBO UŽDUOTIS:

Ištirti elektroninio balsavimo saugumo didinimo galimybes

Analizuoti ir formuluoti reikalavimus elektroninio balsavimo sistemų saugumui

Pasiūlyti bei pritaikyti elektroninio balsavimo sistemos saugumo tikrinimo modelį

Baigiamojo darbo rengimo konsultantai:

.....
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

Vadovas

.....
(Parašas)

.....
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

Užduotį gavau

.....
(Parašas)

..... Aurimas Vengalis

.....
(Vardas, pavardė)

..... 2015-10-28

Vilniaus Gedimino technikos universitetas
Fundamentinių mokslų fakultetas
Informacinių technologijų katedra

ISBN ISSN
Egz. sk.
Data-.....-.....

Antrosios pakopos studijų **Informacinių technologijų** programos magistro baigiamasis darbas

Pavadinimas **Saugumo grėsmės ir jų prevencija elektroninio balsavimo sistemose**

Autorius **Aurimas Vengalis**

Vadovas **Egidijus Ostašius**

Kalba: lietuvių

Anotacija

Šio darbo tikslas yra išanalizuoti elektroninio balsavimo saugumo didinimo galimybes. Elektroninis balsavimas, o ypač jo saugumo aspektai, šiuo metu yra aktuali tema, visuomenėje kelianti daug diskusijų.

Darbe aptarti reikalavimai elektroninio balsavimo sistemai bei pasiūlytas saugumo tikrinimo modelis, kuris orientuotas į galutinius vartotojus. Pasiūlytas modelis pritaikytas remiantis realiais Europos Sąjungos šalies pateiktais statistiniais duomenimis ir pagal juos įvertinta keletas iš galimų atakų prieš elektroninio balsavimo sistemą. Darbe pateiktas būdas, kaip detalai išskaidyti galimas atakas, jas įvertinti, bei apskaičiuoti jų kaštus.

Darbą sudaro 7 dalys: įvadas, elektroninės balsavimo sistemos saugumo apatarimas, šiuo metu veikiančių elektroninio balsavimo sistemų analizė, siūlomo modelio aptarimas, modelio pritaikymas, išvados, literatūros sąrašas.

Darbo apimtis - 73 p. teksto be priedų, 13 iliustr., 4 lent., 43 bibliografiniai šaltiniai.

Prasminiai žodžiai: Elektroninis balsavimas, elektroninio balsavimo saugumas, elektroninės sistemos, atakos medys, balsų pirkimas, rinkėjų verifikacija, elektroninio balsavimo reikalavimai

Vilnius Gediminas Technical University
Faculty of Fundamental Sciences
Department of Information Technologies

ISBN	ISSN
Copies No.	
Date-.....-.....	

Master Degree Studies **Information Technologies** study programme Master Graduation Thesis

Title	Security Threats and their Prevention in Electronic Voting Systems
-------	---

Author	Aurimas Vengalis
--------	------------------

Academic supervisor	Egidijus Ostašius
---------------------	--------------------------

Thesis language: Lithuanian

Annotation

The purpose of this thesis is to analyse the security aspects of electronic voting systems. Electronic voting and especially its' safety aspects is a relevant subject which causes lots of discussions in the community.

The thesis discusses raised security requirements and offers a model to find security holes, which is oriented towards end users. The suggested model is applied with real statistical data from a European Union country and aimed towards possible attacks against an electronic voting system. This paper presents a method how to decompose possible attacks, evaluate them and calculate their costs.

The thesis consists of 7 parts: introduction, electronic voting system safety analysis, current electronic voting systems, proposed model, application of proposed model, conclusions, list of references.

Thesis consists of: 73 p. text without appendixes, 13 pictures, 4 tables, 43 bibliographical references.

Keywords: Electronic voting, electronic voting safety, electronic systems, attack trees, vote buying, voter verification, requirements for electronic voting

(Baigiamojo darbo sąžiningumo deklaracijos forma)

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Aurimas Vengalis, 20150453

(Studento vardas ir pavardė, studento pažymėjimo Nr.)

Fundamentinių mokslų fakultetas

(Fakultetas)

Informacinės technologijos, DGTfm-15

(Studijų programa, akademinė grupė)

BAIGIAMOJO DARBO (PROJEKTO)

SĄŽININGUMO DEKLARACIJA

2017 m. gegužės 23 d.

Patvirtinu, kad mano baigiamasis darbas tema „Saugumo grėsmės ir jų prevencija elektroninio balsavimo sistemose“ patvirtintas 2016 m. gruodžio 20 d. dekanų potvarkiu Nr. 417fm, yra savarankiškai parašytas. Šiame darbe pateikta medžiaga nėra plagijuota. Tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos pažymėtos literatūros nuorodose.

Mano darbo vadovas dr. Egidijus Ostašius.

Kitų asmenų indėlio į parengtą baigiamąjį darbą nėra. Jokių įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs (-usi).

(Parašas)

Aurimas Vengalis
(Vardas ir pavardė)

Turinys

IVADAS	12
DARBO AKTUALUMAS	12
1. ELEKTRONINĖS BALSAVIMO SISTEMOS SAUGUMO APŽVALGA	14
1.1. Elektroninės balsavimo sistemos saugumo reikalavimai	17
2. ELEKTRONINIO BALSAVIMO SISTEMA	18
2.1 Elektroninio balsavimo būdai	19
2.2 Reikalavimai elektroninei balsavimo sistemai	19
2.3. Elektroninės balsavimo sistemos kūrimas bei tobulinimas	21
2.4. Balsavimo mechanizmas	22
2.4.1. Elektroniniam balsavimui reikalinga įranga	23
2.4.2. Balsų pirkimas.....	23
2.4.3. Balsų skaičiavimas	24
2.5. Sertifikavimo mechanizmai	24
2.6. Su konfidencialumu susijusi terminologija	26
2.7. Su verifikavimu susijusi terminologija.....	27
3. ŠIUO METU VEIKIANČIOS ELEKTRONINIO BALSAVIMO SISTEMOS.....	28
3.1. Estijos elektroninio balsavimo sistema	28
3.1.1. Estijos balsavimo sistemos schema	29
3.1.2. Verifikacijos mechanizmas	30
3.1.3. Incidentai	31
3.1.4. Statistika	31
3.1.5. Apibendrinimas	32

3.2. Prancūzijos elektroninio balsavimo sistema	33
3.2.1. Prancūzijos elektroninio balsavimo schema	33
3.2.2. Verifikacijos mechanizmas	35
3.2.3. Statistika	35
3.2.4. Apibendrinimas	35
3.3. Norvegijos elektroninio balsavimo sistema	36
3.3.1. Norvegijos balsavimo sistemos schema	36
3.3.2. Verifikacijos mechanizmas.....	37
3.3.3. Statistika	38
3.3.4. Apibendrinimas	38
3.4. Elektroninių balsavimo sistemų analizė	38
 4. SAUGUMO TIKRINIMO MODELIS.....	 40
4.1. Aktoriai (veikėjai)	40
4.1.1. Kenkėjai	41
4.1.2. Rinkėjai	41
4.1.3. Rinkimų organizatoriai.....	42
4.1.4. Su IT susiję asmenys	42
4.1.5. Auditoriai	42
4.1.6. Kyšininkavimas ir papirkinėjimas	42
4.2. Kenkėjo modelis	43
4.2.1. Kenkėjo modelio pritaikymas.....	43
4.3. Modelis	44
4.3.1. Paieška.....	44
4.3.2. Skaidymas	47
 5. MODELIO PRITAIKYMAS	 54
5.1. Paieška	55
5.1.1. Esybės ir atributai	55
5.1.2. Procesai	55
5.2. Skaidymas	56
5.2.1. Vietos Seime pirkimo ataka.....	56
5.2.2. Ataka prieš pasitikėjimą sistema	63

5.3. Palyginimas.....	66
5.4. Prevencija.....	67
6. REZULTATAI IR IŠVADOS	68
LITERATŪROS SĄRAŠAS	70
PRIEDAI.....	74
Priedas A. VGTU 20-osios jaunųjų mokslininkų konferencijos dalyvavimo pažymėjimas.....	74

Paveikslėlių sąrašas

1 pav. Supaprastinta Estijos elektroninio balsavimo schema [27].....	29
2 pav. Supaprastinta Prancūzijos elektroninio balsavimo schema [27].....	34
3 pav. Supaprastinta Norvegijos elektroninio balsavimo schema [27].....	36
4 pav. Siūlomo saugumo tikrinimo modelio principinė schema.....	44
5 pav. Procedūrinio saugumo analizės metodologinio principo esybių diagrama [41].....	46
6 pav. Laiko grafiko pavyzdys [38]	50
7 pav. Detalaus atakos medžio pavyzdys.....	53
8 pav. Papildytas vietos pirkimo Seime atakos medis (dienomis).....	58
9 pav. Estijos elektroninio balsavimo balsų pasiskirstymas pagal valandas [39].....	60
10 pav. Pilnas atakos medis vietos Seime pirkimo atakai	61
11 pav. Vietos pirkimo Seime atakos kaina pagal klastotų balsų skaičių.....	62
12 pav. Atakos prieš pasitikėjimą rinkimų sistema atakos medis.....	65
13 pav. Pasitikėjimo prieš rinkimų sistemą atakos kaina, norint pavišinti atitinkamą balsų skaičių per valandą	66

Lentelių sąrašas

1 lentelė. Skirtingų šalių elektroninio balsavimo savybių palyginimas.....	9
2 lentelė. Skirtingų šalių elektroninio balsavimo identifikavimo būdų palyginimas	40
3 lentelė. Laiko sąnaudos kenkėjo modeliui [38]	51
4 lentelė. Komponentų vietos Seime pirkimo atakai įgyventi kainos [38].....	61

Terminų ir santrumpų sąrašas

E-Voting (angl. *Electronic voting*) – elektroninis balsavimas. Plati sąvoka apimanti visus elektroniniu būdu atiduodamus balsus.

ISO (angl. *International Organization for Standardization*) – tarptautinė standartizacijos organizacija.

GitHub – naršyklėje naudojama versijavimo repozitorija.

EAL (angl. *Evaluation assurance level*) – IT produkto ar sistemos saugumo vertinimo lygis.

CADA (pranc. *Commission d'Accès aux Documents Administratifs*) – administracinių dokumentų prieigos komisija.

eID (angl. *electronic ID*) – elektroninė ID kortelė naudojama Estijoje.

Mini ID – elektroninė ID kortelė naudojama Norvegijoje.

PIN (angl. *Personal identification number*) – asmeninis identifikavimo numeris.

Android – mobiliams aparatams skirta operacinė sistema.

Proxy serveris (angl. *Proxy server*) – tarpinis serveris, dažniausiai naudojamas tapatybės slėpimui..

NUMIC (pranc. *Le numéro d'identification consulaire*) – valstybės išduotas identifikacinis numeris.

VCS (angl. *Vote collecting server*) – balsų surinkimo serveris.

RCG (angl. *Return code generator*) – atgalinio kodo generatorius.

SMS (angl. *Short message service*) – trumpųjų žinučių paslauga.

NuSMV (angl. *New symbolic model verifier*) – simbolinės modelių verifikacijos atmaina. Patobulinta SMV versija skirta modelių tikrinimui.

PPI (angl. *Pay-per-install*) – mokėk už instaliaciją paslauga.

C&C (angl. *Command and control*) – „valdyk ir kontroliuok“ infrastruktūra skirta sistemų valdymui.

DDoS (angl. *Distributed Denial of Service*) – paskirstytas prieigos prie paslaugos ribojimas.

VPN (angl. *Virtual private network*) – virtualus privatus tinklas.

Botnet – zombių tinklas.

Įvadas

Balsavimas – tai formalus savo nuomonės ar pasirinkimo išreiškimas, kuris atliekamas individo arba grupės individų. Vykstant demokratiniams rinkimams, piliečiai, kurie turi tam teisę, gali balsuoti už siūlomus kandidatus į pozicijas, kurios priklauso nuo rinkimų tipo. Tačiau vykstant rinkimų procesui galimos įvairios klaidos įvairiuose žingsniuose, kaip rinkėjų registravimas, balsų atidavimas ar balsų skaičiavimas. Norint išvengti šių klaidų bei apsisaugoti nuo galimo sukčiavimo, bandoma šiuos procesus automatizuoti kuriant elektronines balsavimo sistemas. Elektroninė balsavimo sistema – tai sistema, kuri padeda organizuoti, administruoti bei vykdyti rinkimų procesus elektroniniu būdu.

Balsavimas yra kertinis bet kokio demokratinio proceso komponentas, todėl visos elektroninės balsavimo sistemos turėtų būti kuriamos remiantis geriausiomis praktikomis. Elektroninis balsavimas leidžia suvokti formalios programų inžinerijos svarbą kuriant sudėtingas sistemas: prastai sukurtos ir prastai dokumentuotos balsavimo sistemos gali turėti rimtų neigiamų pasekmių visiems sistemos veikimu suinteresuotiems žmonėms. Savaimė suprantama, kad formalus elektroninių balsavimo sistemų standartas padėtų spręsti bei aptikti problemas, susijusias su tipine sistemos veikla bei padidintų galutinio produkto patikimumą. Tačiau dar vis nėra visiškai aišku, koks turėtų būti standartas, kad atsvertų daugialypę problemos prigimtį bei susidorotų su šios užduoties sudėtingumu [26].

Elektroninis balsavimas, ko gero, yra vienas iš labiausiai pažeidžiamų saugumo požiūriu procesų, valdomas elektroniniu būdu šiai dienai. Taip yra todėl, nes blogiausiu atveju galintis nutikti scenarijus padarytų didelę įtaką šalies ar net bendrijos politinei sistemai [1]. Šiame darbe bus pamėginta identifikuoti įvairias elektroninio balsavimo saugumo problemas, apžvelgti elektroninio balsavimo siūlomus modelius bei pasiūlyti saugumo tikrinimo modelį, kuris orientuotas į galutinius vartotojus.

Darbo aktualumas

Elektroninis balsavimas gali pasiūlyti nemažai pranašumo lyginant su kitais balsavimo būdais. Elektroninė balsavimo sistema gali būti panaudota bet kuriame balsavimo mechanizmo žingsnyje, kaip balsavimo lapelių dalijimas, balsų surinkimas, analizė ir t. t.

Interneto atsiradimas atvėrė naujas galimybes viešojo sektoriaus reformai, kuomet perkeliant viešąsias paslaugas į elektroninę erdvę ir diegiant 24/7 principą, ėmė keistis institucijų organizacija bei vidinė kultūra.

Pastaraisiais metais tiek Lietuvoje, tiek Vakaruose daug kalbama apie gilėjančias demokratijos problemas:

- Mažėjantį rinkėjų aktyvumą;
- Didėjantį nepasitikėjimą politinėmis institucijomis;
- Politikos virtimą šou.

Šios problemos kelia klausimą apie tradicinių demokratinų mechanizmų efektyvumą ir prasmingumą šiuolaikinėje visuomenėje ir skatina ieškoti naujų piliečių ir valdžios komunikacijos formų, kūrybiškai panaudojant žinių visuomenės teikiamas galimybes [2]. E. demokratijos tikslas yra sustiprinti, išplėsti ir įvairinti piliečių įsitraukimą į valstybės valdymo procesus per efektyvias ir prasmingas internetines diskusijas ir dvipusį informacijos pasikeitimą, sprendžiantį viešojo sektoriaus problemas [3].

Vis daugiau yra kalbama ir apie galimybę dalyvauti Lietuvos Respublikos Seimo ar Prezidento rinkimuose naudojant naujausias informacines technologijas, balsavimą internetu. Elektroninė demokratija yra būtinybė šioje kompiuterių ir informacinių technologijų eroje. Elektroniniai rinkimai yra ir vienas iš svarbiausių e. demokratijos bruožų. Elektroninis balsavimas yra vienas iš jautriausių saugumui procesas, valdomas elektroninėje aplinkoje [1].

Taip pat tai yra alternatyva žmonėms su negalia [2]. Įdiegus elektroninį balsavimą žmonės su negalia, kurie neturi galimybės ateiti į rinkimų apylinkes, galėtų dalyvauti rinkimuose ir atlikti savo pilietinę pareigą namuose. Taip pat žmonėms, kurie vengia viešumos, tai irgi galėtų būti problemos sprendimas. Taip į visuomeninį gyvenimą būtų įtraukiama daugiau žmonių. Aišku, tai nėra vienintelis balsavimo internetu privalumas.

Yra du pagrindiniai balsavimo internetu privalumai – tai rinkimų kaštų mažinimas ir padidėjęs rinkėjų aktyvumas bei susidomėjimas rinkimais. Kompiuterizuotas balsų skaičiavimas padidins rinkimų efektyvumą, o balsavimas internetu bus patogesnis [2]. Daugeliui internetas asocijuojasi būtent su patogumu ir veiksmų atlikimo greitumu. Todėl pagrįstai manoma, kad šis veiksnys padidins rinkėjų aktyvumą.

Naudojant elektronines technologijas svarbus saugumo aspektas. Neįmanoma 100 % užtikrinti balsavimo internetu sistemos saugumo, bet dabartiniai balsavimo būdai taip pat turi nemažai trūkumų [2].

Tyrimo objektas. Elektroninės balsavimo sistemos saugumas.

Tyrimo tikslas. Ištirti elektroninio balsavimo saugumo didinimo galimybes.

Tyrimo uždaviniai. Siekiant iškelto tyrimo tikslo keliama šie uždaviniai:

1. Analizuoti ir formuluoti reikalavimus elektroninio balsavimo sistemų saugumui;
2. Analizuoti jau naudojamą elektroninio balsavimo sistemas, jų taikymo gerąją praktiką, privalumus ir trūkumus siekiant eliminuoti balsų pirkimo/pardavimo galimybę;
3. Išanalizuoti potencialaus kenkėjo galimybes įvykdyti ataką prieš elektroninio balsavimo sistemą;
4. Pasiūlyti elektroninės balsavimo sistemos saugumo tikrinimo modelį;
5. Pritaikyti saugumo tikrinimo modelį.

Tyrimo metodologija. Pagrindinis tyrimo metodas yra literatūros analizė. Elektroninių balsavimų sistemų saugumas yra specifinė mokslinė sritis, šioje srityje ekspertų rasti sunku. Atlikti apklausą galima klausiant tik apie socialinius elektroninių rinkimų aspektus, todėl buvo pasirinktas būtent informacijos šaltinių analizės metodas.

Aprobacija

Darbas tema „Saugumo grėsmės ir jų prevencija“ pristatytas 20-oje Lietuvos Jaunųjų mokslininkų konferencijoje „Mokslas – Lietuvos ateitis“ (Vilniaus Gedimino technikos universitetas, 2017 m. balandžio 12 d.) (žr. priedas A).

1. Elektroninės balsavimo sistemos saugumo apžvalga

Kaip ir visos elektroninės sistemos, taip ir elektroninės balsavimo sistemos susiduria su rimtomis saugumo problemomis, kaip duomenų perėmimas ar įsilaužimas į pačią sistemą. Elektroninės balsavimo sistemos saugumui turi būti keliama kiek įmanoma aukštesni reikalavimai, nes rinkimai yra vienas svarbiausių nacionalinių prioritetų.

Visą saugumo sistemą galima suskaidyti į tris dalis:

- Vartotojo kompiuterio saugumas – kokių saugumo priemonių turėtų imtis vartotojai, norėdami apsaugoti savo kompiuterius;
- Elektroninės sistemos saugumas – ar pati sistema yra saugi, kokia yra sistemos „nulaužimo“ tikimybė;
- Tinklų saugumas, kuriais keliauja informacija. „Man in the middle“ problema – vartotojų balsai iki balsavimo sistemos keliauja elektroniniais tinklais, kokia yra vartotojo balso perėmimo galimybė, ir kokios priemonės padeda apsisaugoti nuo galimų atakų.

Egzistuoja keletas saugumo aksiomų, kurios pasako, kodėl sistemos negali būti visiškai saugios:

- Neįmanoma eliminuoti rizikos;
- Net ir išsprendę „didžiausią“ saugumo problemą, vis tiek turėsime didžiausią saugumo problemą;
- Sistemos silpnų vietų skaičius yra begalinis [1].

Šios aksiomos pabrėžia, jog kad ir koks būtų sistemos saugumas, visada egzistuos tam tikra rizika, jog šis saugumas bus nepakankamas. Šiuo metu sukurti visiškai saugią balsavimo internetu elektroninę sistemą galima tik teoriškai. Yra įmanoma sukurti saugią balsavimo internetu sistemą, tačiau tai būtų pirmoji saugi, tinkle veikianti sistema kada nors sukurta kompiuterių istorijoje [4]. Dažnai manoma, jog neužtikrinus visiško saugumo bet kokia sistema yra nesaugi, o jos naudojimas negali būti rekomenduojamas, tačiau šio teiginio, kuris galbūt tinka realiam gyvenimui negalima taikyti elektroninei erdvei. Reikia suprasti, jog visiško saugumo sąlyga elektroninėje erdvėje yra neįmanoma, jei yra kalbama apie atvirą internetinę, elektroninę sistemą. Todėl reiktų kalbėti ne apie visiško saugumo būtinybę, o apie maksimaliai įmanomą arba pakankamą elektroninį saugumą. Tik tokiu atveju galima rasti realius sprendimus, kurie padėtų padidinti sistemų saugumą. Taip pat didesnis dėmesys turėtų būti skiriamas elektroninių nusikaltimų prevencijai. Užtikrinti pakankamą elektroninės sistemos saugumą yra įmanoma, tačiau yra sudėtinga ar net neįmanoma sukurti visiškai saugią balsavimo internetu sistemą dėl nuolat kuriamų naujų kenkėjiškų būdų.

Elektroninio balsavimo sistemą galima suskirstyti į smulkesnes dalis ir nagrinėti šių dalių saugumą kaip atskirų sistemos posistemių saugumo problemą. Kiekviena posistemė o kartu ir visa sistema turi atitikti visus saugumo standartus. Į smulkias posistemas suskaldytos sistemos saugumą galima įvertinti patikimiau negu nagrinėjant visą sistemą iš karto.

Elektroninė balsavimo sistema gali susidėti iš šių dalių:

- Pačios sistemos;
- Elektroninės balsavimo sistemos kūrimo bei tobulinimo mechanizmų;
- Elektroninės balsavimo sistemos priežiūros – audito mechanizmų;
- Sertifikavimo mechanizmo;
- Rinkėjų, kurie naudoja sistemą. Rinkėjai turi būti identifikuojami, kad galėtų naudotis balsavimo mechanizmu;
- Ryšio kanalų, kuriais keliauja informacija.

Elektroninės balsavimo sistemos kūrėjų vienas iš pagrindinių uždavinių yra užtikrinti šios sistemos saugumą. Šioje sistemoje saugumas turi būti suvokiamas kaip visų sudedamųjų sistemos dalių ne tik atskiras, bet ir bendras saugumas, nes visos elektroninės balsavimo sistemos dalys yra tarpiai tarpusavyje susijusios. Informacijos saugumas – tai informacijos apsauga nuo daugelio įvairių grėsmių siekiant užtikrinti veiklos nepertraukiamumą, kiek galima sumažinti veiklos riziką ir kiek galima padidinti investicijų grąžą bei veiklos galimybes [5].

Plačiąja prasme kiekvieni rinkimai sudaryti iš keturių skirtingų etapų: registracijos, rinkėjų validacijos, balsavimo ir balsų skaičiavimo. Kompiuteriais pagrįstos balsavimo sistemos turi atitikti daug kriterijų tokių kaip tinkamumas, tikslumas, patikimumas, vartotojo identifikacija, slaptumas ir t. t., kad būtų užtikrinami demokratiški rinkimai, kurie yra laisvi, lygūs ir slapti [5].

Vien techninėmis priemonėmis užtikrinti sistemos saugumo yra neįmanoma. Pati sistema, idealiu atveju, gali būti suprojektuota idealiai apsisaugoti nuo išorinių įsibrovimų, bet visada turi būti imtasi priemonių ir prieš vidines grėsmes:

- Darbuotojų, kuriančių sistemą, papirkimas;
- Darbuotojų atsainus požiūris į saugumą.

Techninėmis priemonėmis gali būti laiduotas ribotas saugumas, todėl jis turėtų būti prižiūrimos tinkamu valdymu ir procedūromis. Nustatant, kuriuos priežiūros metodus taikyti, reikia kruopščiai planuoti ir daug dėmesio skirti detalėms [5].

Labai svarbu yra tinkamai nustatyti, kokie turi būti saugumo reikalavimai. Tik tinkamai sudėliojus prioritetus bei kritinius taškus galimas sėkmingas tikslų siekimas. Remiantis ISO/IEC 27002:2013 standartu yra trys pagrindiniai saugumo reikalavimų šaltiniai:

- Pirmasis šaltinis nustatomas vertinant organizacijos riziką, atsižvelgiant į bendrąją organizacijų veiklos strategiją bei tikslus. Atliekant rizikos vertinimą, įvertinamos turtui (visos organizacijos vertybės) kylančios grėsmės, pažeidžiamumas, jų realizavimo tikimybė bei nustatomas galimas jų poveikis.
- Antrasis šaltinis yra teisiniai, įstatyminiai, reglamento ir sutarčių reikalavimai bei socialinė-kultūrinė aplinka, kuriuos turėtų atitikti organizacija, jos prekybos partneriai, rangovai ir paslaugų teikėjai.
- Trečiasis šaltinis yra ypatingas informacijos apdorojimui taikomas principų, tikslų ir veiklos reikalavimų rinkinys, kurį organizacija sukuria savo veiksams paremti [5].

Toliau kiekviena elektroninės balsavimo sistemos dalis bus apžvelgiama atskirai. Reikia paminėti, jog bus aptariamasi tiek elektroninės tiek internetinės balsavimo sistemos. Internetinę balsavimo sistemą galima priskirti elektroninės sistemos posistemei.

1.1. Elektroninės balsavimo sistemos saugumo reikalavimai

Elektroninės balsavimo sistemos tikslas, saugumo požiūriu, yra užtikrinti, kad saugumas būtų integrali sistemos dalis.

Informacinės sistemos apima operacines sistemas, infrastruktūrą, įstaigos taikomas programas, standartinius produktus, paslaugas, naudotojo patobulintas taikomas programas. Informacijos sistemos, palaikančios veiklos procesą, projektavimas ir įgyvendinimas gali turėti lemiamos reikšmės saugumui. Saugumo reikalavimai turėtų būti identifikuoti ir aptarti iki informacijos sistemų projektavimo ir įgyvendinimo.

Visi saugumo reikalavimai turėtų būti identifikuoti projektinių reikalavimų nustatymo stadijoje, be to, įteisinti, aptarti ir įforminti dokumentais kaip visos vykdomos veiklos informacijos sistemos projekto dalis [5].

Techninė internetinio balsavimo pusė turi būti sukurta ir visapusiškai įvertinta kompetentingų technikos specialistų. Internetinio balsavimo sistema turi būti apsaugota nuo visų žinomų ir įmanomų įsilaužimo, klastojimo būdų ar kitokio kompromitavimo [6].

Tenka pažymėti, jog šis reikalavimas nėra įgyvendinamas dėl vienos paprastos priežasties – internetinio balsavimo sistema nėra uždara sistema, todėl neįmanoma jos apsaugoti nuo visų įmanomų grėsmių:

Kad ir kokia gera būtų sistema ji niekaip negalės kontroliuoti šios sistemos vartotojų kompiuterių.

Tobulėjant technologijoms tobulėja ir įsilaužimo, klastojimo būdai, todėl nuo kiekvieno jų apsisaugoti yra neįmanoma, nes nėra galimybės susekti jų atsiradimo.

Šiuo atveju galima užtikrinti tik vienos sistemos dalies saugumą. Rinkėjų kompiuterinio raštingumo lygis turi būti pakankamai aukštas, kad jie galėtų patys tinkamai pasirūpinti savo kompiuteriu saugumu.

Elektroninio balsavimo sistemai galime kelti tokius saugumo reikalavimus [24]:

- Sistemos vientisumas – sistema turi būti apsaugota nuo klastojimo. Idealiu atveju vykstant balsavimo procesui sistemos pakeitimai turi būti uždrausti;
- Duomenų vientisumas bei patikimumas – visi duomenys susiję su balsų įvedimu bei skaičiavimu turi būti vienodo formato;
- Sistemos vartotojų autentikacija – visi asmenys susiję su rinkimų organizavimu ir turintys teisę prisijungti prie sistemos turi pereiti ne trivialų autentikavimo procesą. Neturi būti galimybės jo apeiti net ir užsiimant sistemos priežiūra ar diegimu;
- Sistemos atskaitomybė – visos vidinės operacijos privalo būti stebimos tokiu būdu, kad nepažeistų balsuotojo anonimiškumo. Turi būti galimybė stebėti visas balsų įvedimo ir skaičiavimo operacijas bei atliktas programavimo ir administravimo operacijas;
- Sistemos prieinamumas – sistema turi būti apsaugota nuo tiek atsitiktinių, tiek kenkėjiškų DDoS atakų. Ji privalo būti prieinama visada, kai tai yra numatyta;
- Sistemos patikimumas – sistemos kūrimo metu turi būti stengiamasi kiek įmanoma sumažinti sistemos klaidų tikimybę.

2. Elektroninio balsavimo sistema

Šiame skyriuje bus aptariami elektroninio balsavimo būdai, reikalavimai elektroninei balsavimo sistemai, elektroninės balsavimo sistemos kūrimas bei tobulinimas, elektroninio balsavimo sistemos priežiūra, rinkėjų identifikavimo mechanizmai bei kitos su elektroninių balsavimo saugumu susijusios temos.

2.1 Elektroninio balsavimo būdai

Elektroniniu balsavimu yra vadinamas toks balsavimas, kurio metu balsuojama naudojant elektronines priemones [7]. Galima išskirti du elektroninio balsavimo būdus, tai balsavimas rinkimų apylinkėse naudojant atitinkamą elektroninę įrangą, pvz., lietimui jautrius monitorius, ir nuotolinis balsavimas internetu. Pirmasis iš būdų reikalautų daug investicijų ir kompiuterinė technika reikalautų nuolatinės priežiūros.

Balsavimas internetu – nuotolinis e. balsavimo būdas, kai rinkėjas gali išreikšti savo valią rinkimuose ar referendume naudodamasis interneto ryšiu savo namuose, darbo vietoje ar kitur, kur yra interneto prieiga [6].

Lietuvoje, manome, nėra tikslinga rinktis elektroninį balsavimą rinkimų apylinkėse. Tokiam balsavimui reikėtų rinkimų apylinkėse pastatyti kompiuterius su jautriais monitorių ekranais, pasirūpinti balsų apdorojimo programos įdiegimu. Tačiau kompiuterinė įranga yra brangi, o morališkai ji greitai pasensta [8].

Daug efektyvesnis elektroninio balsavimo būdas būtų balsavimas internetu. Tada kiekvienas gyventojas turintis kompiuterį su interneto prieiga, galėtų dalyvauti rinkimuose neišeidamas iš namų. Tačiau šis būdas yra ir labiausiai pažeidžiamas.

2.2 Reikalavimai elektroninei balsavimo sistemai

Balsavimas internetu turi atitikti tuos pačius reikalavimus kaip ir balsavimas rinkimų apylinkėse:

- Slaptas balsavimas: rinkėjai balsuoja asmeniškai ir slaptai. Kontroliuoti rinkėjų valią rinkimuose yra draudžiama [9].
- Rinkėjo asmenybės nustatymas: reikia tiksliai nustatyti rinkėjo tapatybę.

Atsižvelgiant į šiuos reikalavimus turi būti priimti atitinkami sprendimai, kurie juos užtikrintų ir balsuojant internetu.

Visų pirma elektroninio balsavimo sistema turi tiksliai identifikuoti rinkėją. Tam sistemoje būtų galima realizuoti skaitmeninio parašo mechanizmo palaikymą. Lietuvoje skaitmeninio parašo Įstatymas buvo priimtas 2000 m. liepos 11 d., kuris „reglamentuoja elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, nustato sertifikavimo paslaugas ir reikalavimus jų

teikėjams bei elektroninio parašo priežiūros institucijos teises ir funkcijas“ [10]. Elektroninio balsavimo sistema turi gebėti apdoroti tokį parašą.

Elektroninė sistema taip pat privalo užtikrinti rinkėjo anonimiškumą. Rinkėjo tapatybė neturi būti atskleista. Elektroninėje balsavimo sistemoje rinkėjo anonimiškumo užtikrinimo schema yra panaši į balsavimo paštu schemą, tik atitinkamai perkelta į elektroninę erdvę.

Balsavimo paštu schema [11]:

Rinkėjas balsuoja asmeniškai ir slapta:

- užpildo rinkimų biuletenius;
- užpildytus rinkimų biuletenius įdeda į vidinį balsavimo paštu voką;
- užklijuoja vidinį voką;
- vidinį voką kartu su rinkėjo pažymėjimu įdeda į išorinį voką;
- užklijuoja išorinį voką.

Elektroninio balsavimo sistema turi būti kuo paprastesnė. Kadangi balsavimas vyks internetu, sąsaja tarp sistemos ir jos vartotojo irgi turi būti kuo paprastesnė. Vartotojo aplinka turi būti lengvai suprantama. Rinkėjui naudojantis elektroninio balsavimo sistema neturi kilti dviprasmiškų asociacijų, sistemoje viskas turėtų būti vienareikšmiška ir suprantama.

Net jei viskas veikia gerai gali iškilti balsų perskaičiavimo problema [12]. Iš tiesų juk elektroninėje erdvėje vykstančiuose rinkimuose balsai yra sumuojami naudojant skaičiavimo mašinas, todėl balsų perskaičiavimas neįmanomas. Šioje vietoje atsakomybė tenka elektroninės balsavimo sistemos kūrėjams, kurie kūrė ir testavo šią sistemą, tačiau jei sistema yra sukurta ir ištestuota gerai, tai tuo pačiu turi reikšti, jog ji veikia korektiškai. Žmogiškojo faktoriaus skaičiuojant balsus čia nelieta, todėl apeliacijos turėtų būti atmetamos, juk vienintelis būdas patikrinti, ar gerai suskaičiuojami balsai, tai tikrinti elektroninės balsavimo sistemos programinį kodą, o ne balsus, kita vertus jei sistema funkcionuoja gerai, automatinis balsų skaičiavimo mechanizmas bus tikslesnis ir efektyvesnis nei rankinis skaičiavimas. Dėl to paties žmogiškojo faktoriaus nebuvimo nelieta ir žmogiškųjų klaidų, kurios vėlgi gali būti padarytos tiek tyčia, tiek netyčia.

Aišku nėra programinės įrangos be klaidų, todėl reikia būtinai užtikrinti, jog klaidos būtų per trumpiausią įmanomą laiką ištaisytos, o balsų skaičiavimo algoritmas paleistas iš naujo. Rinkėjų elektroniniams balsavimo biuleteniems nieko neturi atsitikti, jei jie buvo tinkamai išsaugoti duomenų

bazėje. Norint ištaisyti kuo daugiau programinės įrangos klaidų reikia, kad šią programinę įrangą testuotų kuo daugiau žmonių. Tai galima įgyvendinti padarant programos kodą viešai prieinamu. Taip galima išspręsti ir žmonių nepasitikėjimo informacine sistema problemą. Kai eilinis vartotojas galės pats pažiūrėti programinės įrangos, kuria vartotojas naudojasi, kodą jis galės pats nuspręsti kiek saugi yra elektroninio balsavimo sistema. Ir tuo pačiu, jei ras elektroninėje balsavimo sistemoje saugumo spragų galės apie jas pranešti. Pavyzdžiui, Estijoje savo naudojamos elektroninės balsavimo sistemos išeities kodą paviešino GitHub svetainėje (nuoroda į kodą literatūros sąrašė) [13].

Kai buvo pradėta kurti elektroninio balsavimo sistema Šveicarijoje, buvo baiminamasi, jog ši sistema gali padidinti elektroninę atskirtį tarp vartotojų, taip dar labiau padidindama atskirtį tarp nepasiturinčiųjų, kurie neturi nei kompiuterio, nei prieigos prie interneto, ir tarp pasiturinčiųjų gyventojų, kurie galės pasirinkti ar balsuoti patogesniu elektroniniu būdu ar ne [14]. Ši problema aktuali labiau nepasiturinčioms šalims, kuriose atskirtis tarp pasiturinčių ir nepasiturinčių gyventojų yra didelė. Labiau išsivysčiusiose šalyse problema nėra aktuali, nes gyventojų turinčių asmeninį kompiuterį su priejimu prie interneto sparčiai daugėja.

Labai svarbus yra galimo elektroninio nusikaltimo prevencijos klausimas. Juk naudingiau, kad nusikaltimas neįvyktų, nei turėti labai geras ar tobulas priemonės tam nusikaltimui išaiškinti.

2.3. Elektroninės balsavimo sistemos kūrimas bei tobulinimas

Elektroninio balsavimo sistemos, kaip ir bet kokios kitos elektroninės sistemos, niekada nebus visiškai saugios vien dėl tos priežasties, kad pačios sistemos turi nuolat vystytis, jog patenkintų vis naujus vartotojų poreikius. Jei sistema yra nuolat besivystanti, tai ir sistemos saugumas turi būti nuolat vystomas. Todėl tokių sistemų priežiūra yra brangi, joms reikalingas nuolatinis testavimas, o kiekvieno papildomo saugumo sluoksnio pridėjimas yra tik laiko klausimas. Juk svarbu užkirsti kelią nusikaltimui ir padaryti viską, kad rinkimai vyktų saugiai. Elektroniniai rinkimai yra ypatinga sritis, kur įvykus nusikaltimui ir sužlugdžius elektroninį balsavimą, nuostoliai gali būti milžiniški, o kai kuriais atvejais, ypač, jei klaidinantys balsai bus įskaityti, gali įvykti nacionalinio masto katastrofa.

Todėl vis dažniau rengiamos ne tik su elektroniniu saugumu siejamos tarptautinės konferencijos, bet yra rengiamos ir tiesiogiai su elektroninio balsavimo aspektais susijusios konferencijos.

Vokietijoje yra kuriama elektroninių balsavimo sistemų vertinimo ir sertifikavimo bazė vadinama – bendrų kriterijų saugumo forma (angl. *Common Criteria Protection Profile*). Šioje formoje yra

apibrėžiami pagrindiniai reikalavimai nuotolinėms elektroninėms balsavimo sistemoms. Reikalaujama, kad saugumo forma žemesnio lygio tarp universitetiniuose rinkimuose būtų bent (EAL2+) lygio. Aukštesnio lygio rinkimams rekomenduojama saugumo lygį atitinkamai koreguoti. [15]

EAL – (angl. *Evaluation assurance level*) įvertinimo garantijos lygmuo. Įvertinimo garantijos lygmenys gali kisti nuo 1 iki 7+, kur 7 reiškia patį griežčiausią vertinimą. Pavyzdžiui saugumo forma EAL 2+ charakterizuojama tokiais aspektais:

- Vertintojas vykdo struktūrinius ir nepriklausomus testus;
- Dokumentacijos dizaino ir vartotojo sąsajos analizė vykdoma aukščiausiu lygmeniu;
- Funkcijų analizė;
- Vertintojas turi vykdyti aiškiausiai numanomų sistemos spragų paiešką;
- Sistema turi turėti atskirą konfigūravimo posistemę;
- Turi būti saugaus sistemos pristatymo įrodymai [16].

EAL2+ saugumo kriterijus yra pakankamas vykdyti elektroninius rinkimus mokyklų, asociacijų, universitetų lygmenyje, tačiau Seimo rinkimuose reikia aukštesnių kriterijų [17].

Akivaizdu, jog sistemos kūrimas apima ne tik paties programinio kodo rašymą, bet ir elektroninio balsavimo sistemos perdavimą, testavimą. Turi būti aiškiai aprašytos priėmimo testų procedūros.

2.4. Balsavimo mechanizmas

Elektroninė erdvė įprastiems vartotojams tampa vis pavojingesnė. Sparčiai daugėja elektroninių virusų, privačius duomenis bandoma apgaulės būdu išgauti iš vartotojų. Bet nepaisant to noras naudotis elektroninės erdvės teikiamais privalumais tik didėja, tai skatina įvairių antivirusinių programų tobulinimą, bei didesnius saugumo reikalavimus internetinėms naršyklėms.

Yra daug įvairių būdų kaip elektroninėje erdvėje išgauti vartotojo slaptą informaciją, pagrinde prisijungimo vardus ir slaptažodžius, kurie naudojami prisijungimui prie įvairių elektroninių sistemų. Taip pat atakos gali būti nukreiptos ne tik prieš vartotojus, bet ir prieš elektronines sistemas, kuriomis vartotojai naudojasi, taip blokuojant šių sistemų darbą.

2.4.1. Elektroniniam balsavimui reikalinga įranga

Rinkėjai arba elektroninės balsavimo sistemos vartotojai yra ta grupė į kurią ir yra orientuota sistema. Tačiau, kad ir kokia saugi būtų elektroninio balsavimo sistema už rinkėjo kompiuterio saugumą ji negali atsakyti, todėl visų pirma patys rinkėjai turi būti suinteresuoti apsaugoti savo kompiuterius.

Techninę įrangą balsavimui įsigyti nėra sudėtinga. Norint balsuoti internetu Estijoje reikia turėti kompiuterį, kuris būtų prijungtas prie interneto ir kortelių skaitytuvą, jei balsuojama naudojantis specialiomis kortelėmis, kuriose įmontuota mikroschema su elektroninio parašo mechanizmu. Į tokį kortelių skaitytuvą yra įdedama Estijoje naudojama ID kortelė, kuria generuojamas unikalus skaitmeninis parašas [18].

Programinę įrangą reikalingą balsavimui vartotojas gali nemokamai parsisiųsti, tačiau šios įrangos saugumą, jau turi užtikrinti kompiuterio naudotojas.

2.4.2. Balsų pirkimas

Kaip jau buvo rašyta, norint iš rinkėjo nupirkti jo balsą galima, arba jam sumokėti ar kitaip jį paveikti, kad pastarasis balsuotų už atitinkamą kandidatą arba gauti iš rinkėjo jo prisijungimo prie elektroninės balsavimo sistemos duomenis ir tada balsuoti už pastarąjį.

Pirmu atveju balso pirkėjas turi būti tikras, kad rinkėjas balsavo taip kaip buvo liepiamas. Antru atveju kai įsigijami prisijungimo duomenys, pirkėjas pats balsuoja už rinkėją ir yra užtikrintas, kad balsuota taip kaip reikia.

Ši problema elektroninėse balsavimo sistemose gali būti nesunkiai išspręsta leidžiant balsuoti rinkėjui keletą kartų ir užskaitant tik paskutinį balsą. Tokiu būdu balso pirkėjas negalės būti tikras, jog rinkėjas vėliau neperbalsuos. Elektroniniuose rinkimuose skirtingai negu elektroninėje komercijoje vartotojas negali atsispausdinti jokio dokumento, kuriuo galėtų vėliau įrodyti savo teisumą [19].

Nors balsų pirkimo ar pardavimo problema buvo aktuali ir anksčiau, elektroninio balsavimo atveju reikia įdėti dar daugiau pastangų, norint jos išvengti. Elektroninė erdvė šiuo atžvilgiu padidina balsų pirkėjų galimybes, pvz., galima pirkti balsus internetu, o ne prie rinkimų apylinkės, tačiau tinkamai panaudojant elektroninės erdvės galimybes galima maksimaliai sumažinti balsų pirkimą ar pardavimą. Šiuo atveju viskas priklausys nuo rinkėjo pilietiškumo jausmo ar jis panorės, visų pirma, parduoti savo balsą, o visų antra, ar norės pasinaudoti galimybe pakeisti savo parduotą balsą.

2.4.3. Balsų skaičiavimas

Suskaičiuoti elektroninio balsavimo rezultatus nėra sudėtinga, tačiau aktuali yra balsų perskaičiavimo problema. Kaip patikrinti, ar elektroninė balsavimo sistema nepadarė klaidos skaičiuodama balsus. Tokiam atvejui turi būti įdiegtas specialus balsų patikrinimo mechanizmas, kad rinkėjas galėtų pats patikrinti, ar jo balsas buvo užskaitytas sėkmingai.

Rinkėjas balsavęs, pavyzdžiui, galėtų atsispausdinti užkoduotą pranešimą arba, jei balsavimas vyksta rinkimų apylinkėje, elektroninėmis balsavimo mašinomis, šios galėtų atitinkamą pranešimą atspausdinti. Rinkėjas bet kada galėtų prisijungęs prie rinkimų organizatorių tinklapio patikrinti, ar jo balsas buvo užskaitytas sėkmingai. Kadangi elektroniniu būdu galima balsuoti kiek norima kartų, užkoduoti pranešimai visada bus skirtingi ir rinkėjas galės atsispausdinti kiek pageidauja užšifruotų pranešimų. Taip pat galima sudaryti galimybes, kad asmuo ar kokia nors viešoji įstaiga galėtų gauti šifruotus balsus, juos su specialia programine įranga dešifruoti ir perskaičiuoti, taip galima įsitikinti, kad balsų dešifravimo ir skaičiavimo mechanizmas veikia korektiškai [20].

Toks balsavimo mechanizmas ne tik užtikrintų didesnę skaidrumą, bet ir padidintų rinkėjų pasitikėjimą elektroninio balsavimo sistema. Tačiau, vėlgi reikia nepamiršti užtikrinti, kad rinkėjas išlaikytų savo anonimiškumą.

2.5. Sertifikavimo mechanizmai

Sertifikavimas – procedūra, kuria sertifikavimo įstaiga pripažįsta, kad produktas, procesas, paslauga, fizinio asmens kvalifikacija atitinka nustatytus reikalavimus. [22] Iš šio sertifikavimo apibrėžimo matome, jog norint turėti sertifikuotą sistemą reikia:

- Aprašyti sertifikavimo procedūras;
- Sudaryti sutartį su sertifikavimo įstaiga;
- Programinę įrangą bei procedūras turi atitikti nustatytus reikalavimus.

Kaip matome, sertifikuotos turi būti visos procedūros, elektroninio balsavimo atveju tai būtų ir rinkėjo identifikavimo procedūra ir balsų skaičiavimo procedūra ir kitos naudojamos procedūros.

Kitas svarbus saugumo aspektas yra sertifikuojančios įstaigos parinkimas bei sertifikavimo rezultatų viešinimas. Jei parinkta sertifikuojanti įstaiga bus iš privataus sektoriaus, tai sertifikavimo rezultatų paskelbimas gali būti prieinamas tik siauram specialistų ratui, nes rezultatų paviešinimas visuomenei gali

kirstis su sertifikuojančios įmonės vidaus taisyklėmis arba saugumo politika. Kaip kad įvyko Prancūzijoje 2006 metais, kai visuomenės atstovai pareikalavo sertifikavimo ataskaitų pavišimo [23]. 2006 Prancūzijos vidaus reikalų ministerija atsisakė patenkinti tokį prašymą motyvuodama kriterijais, kuriuos gavo iš CADA (pranc. *Commission d'Accès aux Documents Administratifs*). CADA yra patariamasis organas, kurio tikslas yra nustatyti kokie dokumentai gali būti prieinami visuomenei, o kokių peržiūrėti negalima ir su šiais dokumentais turi būti atitinkamai elgiamasi. Šis organas rekomendavo neviešinti prašomos informacijos argumentuodama tuo, kad ši informacija gali pakenkti komercinėms ir industrinėms paslaptims, o tai savo ruožtu gali pakenkti teisingiems ir nešališkiems rinkimams [23].

Visuomenė tikrai norės žinoti, ar tokios svarbios sistemos sertifikavimas įvyko sėkmingai. Bet jeigu sertifikavimą atliks privati kompanija, ataskaitos galės būti prieinamos tik ribotam ratui specialistų. Jei sertifikavimą atliks vieša įstaiga, visuomenė gali pradėti įtarti, jog sertifikavimo procesas galėjo vykti neskaidriai.

Sertifikuoti reikia ne tik programinę įrangą, bet ir techninę jos dalį. Kiekvienas kompiuteris, jei balsuojama rinkiminėse apylinkėse, naudojant kompiuterinę techniką, turi būti patikrinta. Taip pat sertifikavimas įtakoja ir serverius, kuriuose bus saugoma visa informacija, turi būti užtikrintas jų saugumas, kad visų rinkimų metu techninė įranga negali būti koku nors būdu derinama, išskyrus tuos atvejus, kai įvyksta koks nors gedimas. Gedimo atveju turi būti aprašytos atitinkamos elgesio procedūros. Priešingu atveju jei įvyks koks nors pakeitimas, bus labai sunku įrodyti, jog tai buvo padaryta legaliai ir nebuvo pažeistos saugumo procedūros.

Šie techniniai elektroninių įrenginių nesklandumai buvo pastebėti ir išaiškinti vien dėlto, kad jų sukeltų klaidų padariniai buvo dideli ir lengvai pastebimi. Ką galima padaryti ir kaip aptikti klaidas, jei jos nebuvo tokios didelės ir jų padariniai nėra taip lengvai matomi. Kita vertus, jei rinkimai vyksta įprastiniu būdu ir balsai skaičiuojami rankiniu būdu, tai visada egzistuoja ir žmogiškos klaidos tikimybė, todėl tiek vienu, tiek kitu būdu skaičiuoti balsus nėra visiškai patikima ir visada egzistuoja klaidos tikimybė.

Sertifikuojant elektroninę balsavimo sistemą Prancūzijoje ji turi atitikti 114 įvairiausių kriterijų. Šis pavyzdys parodo, jog sertifikavimo procesas yra tikrai labai svarbi elektroninės balsavimo sistemos dalis.

Tuo tarpu Belgijoje elektroninės balsavimo sistemos išėties tekstai rinkimuose dalyvaujančioms partijoms yra duodami dar prieš rinkimus, tiesa partijos turi laikytis tam tikro konfidencialumo susitarimo, o po rinkimų šie išėties tekstai yra paskelbiami viešai, tačiau elektroninio balsavimo sertifikavimo išvados nėra taip lengvai prieinamos [36]. Kodėl sertifikavimo išvados yra labiau

saugomos negu pačios elektroninės sistemos išeities tekstai? Visų pirma norint suprasti išeities tekstus reikia turėti aukštą IT išsilavinimą, bei turėti programavimo patirties ar bent kažkiek būti susipažinus su programavimo pagrindais, be to reikia išmanyti konkrečias technologijas, kurios yra naudojamos kuriant elektroninę balsavimo sistemą. Dėl šios priežasties nėra baiminasi paskleisti išeities tekstus, be to šis veiksmas suteikia pasitikėjimo rinkėjams balsavimo mechanizmo skaidrumu. Tuo tarpu sertifikavimo išvados jau bus suprantamos kur kas platesniam rinkėjų ratui. Jos gali būti netinkamai interpretuotos ir gali sukelti priešišką reakciją, aišku tik tuo atveju jei šios išvados yra neigiamos. Dėl šio priežasties svarbu tinkamai parinkti ratą piliečių, kurioms šios išvados bus prieinamos.

Tuo tarpu Estijos elektroninė balsavimo sistema neturi jokių formalių sertifikavimo procedūrų. 2007 metais Estijos elektroninė balsavimo sistema buvo keletą kartų tiriama specialistų, tačiau šių specialistų ataskaitos nebuvo pavišintos. Sertifikavimo procesas kaip rodo šis pavyzdys nėra privalomas, tačiau šis procesas suteikia elektroninio balsavimo sistemai papildomo saugumo todėl būtų natūralu, jei elektroninės balsavimo sistemos būtų sertifikuojamos. Taip pat rinkimų laikotarpio metu buvo atliekamas privatus auditas, kuris turėjo patikrinti ar visais naudojamais protokolais buvo tinkamai naudojasi, tačiau šio audito išvados taip pat nebuvo pavišintos. Norint, jog sistema būtų pasitikima reikia, jog sistemos sertifikavimo ar audito rezultatai būtų prieinami bent siauram ratui rinkėjų, taip bus sprendžiama ne vien tik pasitikėjimo problema, bet tokiu būdu būtų galima ir kontroliuoti sistemos veiklą [25].

2.6. Su konfidencialumu susijusi terminologija

Su konfidencialumu susijusi terminologija šiame darbe apibūdinama remiantis tuo momentu laike, kai kenkėjas (balsų pirkėjas ar pan.) gali komunikuoti su rinkėju. Rinkėjas gali būti kenkėjo įtakos sferoje aktyviai, pvz. jam yra daromas spaudimas, jam yra grasinama arba rinkėjui gali tiesiog nerūpėti. Rinkėjas taip pat gali būti kenkėjo įtakos sferoje to net nesuprasdamas. Keletas svarbių terminų, susijusių su elektroniniu balsavimu:

- Balso privatumas (angl. *ballot-privacy*) – užtikrina, jog vien tik viešai prieinamais duomenimis bei kanalais, joks išorinis asmuo nesužinos už ką balsavo individualus rinkėjas [28];
- Patvirtinimo nebuvimas (angl. *receipt-freeness*) – užtikrina, kad balsą atidavęs rinkėjas neturi kaip įtikinti kenkėjo už ką jis balsavo ar už ką atidavė savo paskutinį balsą, laikantis sąlygos, kad kenkėjas gali matyti visas žinutes tarp rinkėjo naudojamos aplikacijos ir rinkimų sistemos bei,

kad kenkėjas turi visą viešai prieinamą informaciją. Kenkėjas gali kontaktuoti su rinkėju prieš ir po balsavimo procesą, kurio metu rinkėjas gali atskleisti savo konfidencialią informaciją. Norima pabrėžti, kad kenkėjas gali komunikuoti su rinkėju prieš ir po balsavimo, tačiau ne balsavimo proceso metu. Šitaip įgalinamas balso slaptumas (konfidencialumas). Trumpai tariant apibrėžimas sako, jog neįmanoma įrodyti už ką rinkėjas balsavo [28].

- Atsparumas spaudimui (angl. *coersion resistant*) – spaudimui atspari rinkimų sistema leidžia korupcijos kontekste įgalinti ne tik balso patvirtinimo nebuvimą, bet ir saugo nuo atsitiktinumų, simuliacijų bei balsų gadinimo. Šio apibrėžimo ribose kenkėjas gali turėti kontaktą su rinkėju prieš, per ir po balsavimo procesą ir gali atskleisti jo asmeninius duomenis prieš balsavimo procesą. Kenkėjas gali priversti ar įtikinti rinkėją tyčia sugadinti savo balsą arba balsuoti atsitiktiniu būdu arba net priversti rinkėją atiduoti savo prisijungimo duomenis kenkėjui, kuris prabalsuos jo vardu [29].
- Prievartos (įtakos) įrodymas – apibrėžiama, kaip informacijos apie korupcijos įvykius turėjimą ir jų įtraukimą į rinkimų išvadas. Atsakingi asmenys, prižiūrėtojai bei rinkėjai gali peržiūrėti šią informaciją ir ją panaudoti norint nustatyti ar rinkimų rezultatai tinkami suteikti mandatą laimėjusiam kandidatui. Iš to seka, kad rinkimų organizatoriai pagal šiuos duomenis gali nuspręsti ar laikyti rinkimus galiojančiais (įvykusiais) [30].
- Besąlygiškas privatumas – jokiais būdais neįmanoma nustatyti už ką rinkėjas balsavo. Prieš tai minėtuose apibrėžimuose yra įmanoma sužinoti už ką rinkėjas balsavo iššifravus jo balsą, tačiau statistikose tokia informacija nėra įtraukiama. Šis apibrėžimas pažymi, jog net balsų skaičiavimo ar saugojimo procese rinkėjas nėra susietas su atiduotu balsu [31].

2.7. Su verifikavimu susijusi terminologija

Egzistuoja aiški priešprieša tarp balso patvirtinimo nebuvimo ir balsavimo sistemos atsparumo spaudimui, t. y. abu sprendimai vienas kitą šiek tiek priešina. Toliau bus aptarta su verifikavimu susijusi terminologija:

- Individuali verifikacija – leidžia rinkėjui patvirtinti, jog jo balsas pasiekė rinkimų organizatorių arba pamatyti, kaip jo balsas įtakojo galutinį rinkimų rezultatą [28].

- Universali verifikacija – teisingiems rinkimams užtikrinti nepakanka taikyti tik individualią verifikaciją. Universali verifikacija apibrėžiama kaip „kiekvienas gali patvirtinti, jog paskelbti rinkimų rezultatai yra tiksli suma visų individualių balsų“ [21].

3. Šiuo metu veikiančios elektroninio balsavimo sistemos

Pagal VKA [26] atliktą tyrimą, šiuo metu iš viso 11 šalių bandė įdiegti elektroninį balsavimą, iš kurių 4 jį sustabdė. Likusios 7 šalys yra Australija, Kanada, Estija, Prancūzija, Indija, Norvegija ir Šveicarija. Elektroninio balsavimo diegimo priežastys skiriasi tarp skirtingų šalių, priklausomai nuo to, kokiam balsuojančiųjų tipui sistema yra pritaikoma, pavyzdžiui, Prancūzija siekia padidinti išeivijos balsuojančiųjų skaičių, o Estija nori padidinti dažniausiai balsuojančiųjų skaičių (kurie kartais balsuoja), o ne tų, kurie niekad nebalsuoja [26].

Sekančiuose poskyriuose bus aptartos skirtingos elektroninio balsavimo schemas, kurios pritaikytos Estijoje, Prancūzijoje bei Norvegijoje.

Schemas pasirinktos pagal prieinamą informaciją ir pagal tai, jog jos šiuo metu naudojamos bei tai, jog Europos šalių balsavimo modelis yra artimesnis Lietuvos modeliui nei pvz., rytų šalių.

3.1. Estijos elektroninio balsavimo sistema

Estija pristatė elektroninį balsavimą 2005 metais ir nuo tada fiksuoja vis gausesnę naudojimąsi sistema. Iki Estijai pritačius elektroninį balsavimą, jokia kita šalis nebuvo bandžiusi elektroninio balsavimo tokiu dideliu mastu. Dėl to buvo investuota daug pastangų projektuojant sistemą, ypač tam, kad sumažinti balsų pirkimo tikimybę. Estijos elektroninio balsavimo sistema buvo pirmoji, kuri leido perbalsuoti (įskaitomas tik paskutinis balsas). Estijos balsavimo periodas susideda iš [42]:

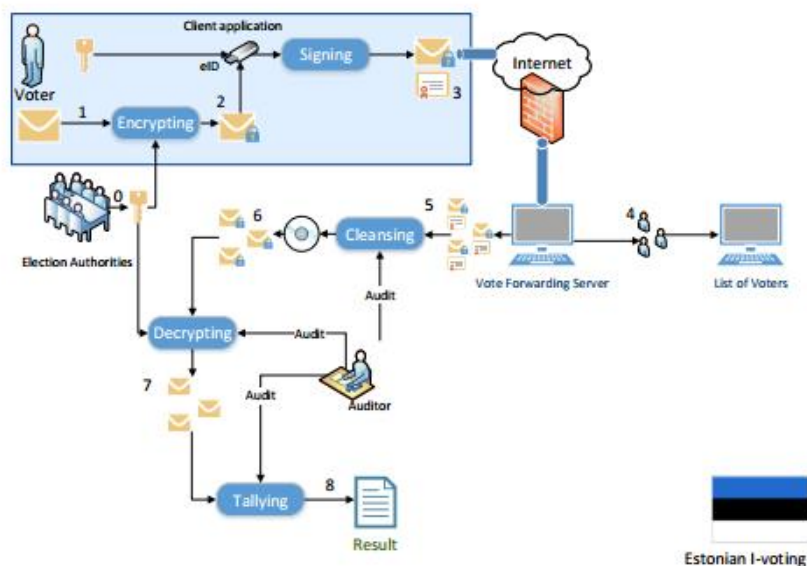
- Pirmas septynias rinkimų periodo dienas galima iš anksto balsuoti bei perbalsuoti internetu, taip pat ir balsuoti vietinėse apylinkėse;
- Trys dienos skirtos balsų skaičiavimui;
- Išaušus rinkimų dienai, visi kurie dar nebalsavo gali tai atlikti rinkimų dieną.

Perbalsuoti internetu galima bet kiek kartų, tačiau perbalsuoti įprastu būdu galima tik kartą. Balsuojant įprastu būdu anuliuojami visi prieš tai rinkėjo internetu atiduoti balsai. Žmonių balsavusių

internetu sąrašas yra išsiunčiamas į balsavimo stotį dieną po to, kai baigiasi balsavimo internetu periodas taip pat pažymint visus, kurie balsavo įprastu būdu. Jei žmogus perbalsavo įprastiniu būdu, jo internetu atiduoti balsai yra anuliuojami prieš atliekant elektroniniu būdu atiduotų balsų skaičiavimą. [27]

3.1.1. Estijos balsavimo sistemos schema

Estijos elektroninio balsavimo sistemą gamino Estų įmonė „Cybernetica“ ir supaprastintas jos veikimas apibūdintas toliau. Kiekvienas Estijos pilietis yra įpareigotas turėti naujo formato elektroninę ID kortelę (eID), kuri turi įmontuotą išmaniąją kortelę, gebančią šifruoti informaciją bei ją pasirašyti. Rinkėjai parsisiunčia balsavimo aplikaciją į savo kompiuterį, įdeda savo eID kortelę į kortelių skaitytuvą ir autentikuoja save su išmaniąja kortele įvesdami savo asmeninį PIN kodą (PIN1). Tada jie aplikacijoje pasirenka savo partiją ar kandidatą ir užšifruoja savo balsą viešuoju raktu, kurį suteikia rinkimų organizatoriai. Tada jie pasirašo užšifruotą balsą dar kartą autentikuodamiesi su išmaniąja kortele ir įvesdami antrą asmeninį PIN kodą (PIN2). 1 pav. pavaizduota autentikacijos procedūra po to, kai rinkėjas jau yra parsisiuntęs aplikaciją į savo kompiuterį. PIN naudojimas nepavaizduotas diagramoje [27].



1 pav. Supaprastinta Estijos elektroninio balsavimo schema [27]

1. Aplikacija yra sukonfigūruota naudoti viešą šifravimo raktą ir geba gauti kandidatų sąrašą;
2. Rinkėjas pasirenka norimą partiją bei kandidatą aplikacijoje;

3. Rinkėjas užšifruoja savo balsą naudodamas rinkimų organizatoriaus suteiktu išoriniu raktu;
4. Rinkėjas pasirašo užšifruotą balsą naudodamasis privačiu išmaniosios kortelės raktu; Užšifruotas ir pasirašytas balsas yra siunčiamas į balsų perdavimo serverį naudojant SSL apsaugotą ryšio kanalą;
5. Rinkėjų asmeninė informacija yra išsaugoma rinkėjų sąrašų serveryje atskirai nuo balsų;
6. Po rinkimų, visi e. balsai yra apdorojami nuimant parašą ir perduodami į balsų tvarkymo procesą, kur sutvarkomi visi pakartotiniai balsai;
7. Užšifruoti ir apvalyti balsai yra įrašomi į kompaktinį diską ir perduodami iššifravimo procesui. Iššifravimo procese naudojamas rinkimų organizatoriaus privatus iššifravimo raktas;
8. Iššifruoti balsai yra perduodami balsų skaičiavimo procesui;
9. Balsų skaičiavimo procesas pateikia galutinius rezultatus.

Įvairūs proceso žingsniai yra audituojami nepriklausomo auditoriaus. Didžiausias dėmesys skiriamas valymo, iššifravimo ir skaičiavimo procesuose.

3.1.2. Verifikacijos mechanizmas

2013 metais Estija pradėjo individualių rinkėjų verifikacijos vietiniams rinkimams, naudojant Android aplikaciją, bandymus. Kai rinkėjas užšifruoja savo balsą išoriniu raktu, į užšifruotą dalį pridedamas atsitiktinis numeris. Rinkimų organizatorių sistema sugeneruoja ir siunčia sesijos kodą į rinkėjo mobiliųjį telefoną (perbalsuojant būtų siunčiamas naujas sesijos kodas). Balsavimo aplikacija tada parodo QR kodą, kuriame saugomas sesijos bei atsitiktinis numeris, kuris gali būti nuskanuotas Android aplikacijos. Tuomet aplikacija identifikuoja save su rinkimų sistema naudodama sesijos kodą, pagal kurį sistema išsiųs kandidatų sąrašą bei užšifruotą balsą atgal į aplikaciją.

Aplikacija tuomet apdoroja gautą informaciją naudodama atsitiktinį numerį bei sesijos kodą ir atvaizduoja rinkėjo išsiųstą balsą. Šiuo metodu negalima visada sužinoti savo paskutinio balso, jis skirtas verifikuoti ar rinkėjo išsiųstas balsas buvo tinkamai užšifruotas ir apdorotas rinkimų sistemos. Kiekvieną kartą perbalsuojant sistema sugeneruos naują sesijos kodą, kuriuo galima verifikuoti atitinkamą atiduotą balsą. Tokiu būdu galima kovoti su balsų pirkimu, užtikrinant, kad paskutinis atiduotas balsas buvo atiduotas tikrojo rinkėjo. Šiuo metodu nėra tikrinama, ar balsas buvo teisingai apskaitytas bendrame rinkimų rezultate [32].

3.1.3. Incidentai

2011 metų parlamento rinkimuose įvyko du incidentai susiję su elektroniniu balsavimu. Pirmas įvyko iššifravimo ir balsų skaičiavimo metu. Vienas balsas negalėjo būti apskaitytas, tačiau buvo teisingai užkoduotas. Tai galėjo įvykti dėl keleto priežasčių [33]:

- Buvo perrašyta ir panaudota nauja balsavimo aplikacija, kuri tinkamai komunikavo su rinkimų sistema, tačiau nekorektiškai suformavo balsą;
- Oficiali aplikacija buvo netinkamai naudojama;
- Oficialioje aplikacijoje buvo klaidų;

Kad sužinoti tikslią priežastį būtų tekę iššifruoti balsą, kas būtų pažeidę anonimiškumo sąlygą. Būtent dėl šios priežasties teismas nusprendė nieko nedaryti. Vėlesni tyrimai atskleidė tik dvi galimas priežastis, dėl to balsas buvo laikomas negaliojančiu:

- Sunkiai aptinkama atminties klaida aplikacijoje;
- Tyčia sugadintas balsas naudojant HTTPS proxy serverį kaip tarpininką.

Šis incidentas taip ir nebuvo iki galo išspręstas ir turbūt niekada nebus.

Antrasis incidentas susijęs su studentu, kuris dekompileavo balsavimo aplikaciją ir įterpė į ją kenkėjišką kodą, kuris pakeisdavo kandidatą už kurį yra balsuojama ir užregistruodavo rinkėjo pirminį pasirinkimą. Pakeista aplikacija užregistruodavo pirminį rinkėjo pasirinkimą, sukurdamo netikrą ekrano atvaizdą ir po juo paslėpdavo visus pelės judesius rinkėjui to nepastebint. Tam padaryti studentas sugaišo 5 dienas.

Kai studentas pareiškė, jog sukūrė šią kenkėjišką aplikaciją saugumo tikrinimo sumetimais, rinkimų organizatoriai deklaravo, jog jie buvo pažymėję visus iš netikros aplikacijos išsiųstus balsus kaip įtartinus. Teismas nusprendė, jog toks mažas kiekis suklustotų balsų neturėjo jokios įtakos, jie buvo anuliuoti ir bendras rinkimų rezultatas buvo įskaitytas [33].

3.1.4. Statistika

Elektroninių balsų skaičius tarp tam teisę turinčių ir rinkimuose dalyvaujančių rinkėjų padidėjo nuo 1.9 % per 2005 metais iki 24.3 % 2011 metais. Taip pat per šį laikotarpį didėjo dalyvaujančių rinkimuose skaičius. Rinkėjų, balsavusių parlamento rinkimuose 2007 metais skaičius padidėjo nuo 61,9 % iki 63,5

% lyginant su 2011 metais, o vietiniuose rinkimuose nuo 47,4 % iki 60,6 % lyginant su 2005 ir 2009 metais [34].

Nepaisant tokių aspektų, kaip politinė situacija ar įdomūs debatai kad pagrįsti padidėjusį rinkėjų aktyvumą, Trechsel and Vassil [39] teigia, remdamiesi simuliacijomis, kad vietiniai rinkimai 2009 metais turėjo apie 2,6 % didesnę aktyvumą nei panašūs rinkimai be elektroninio balsavimo galimybės. Taip pat lyginant balsuojančių internetu savybes su balsuojančių tradiciniu būdu, didelės įtakos nesudarė nei lytis, pajamos, išsilavinimas, gyvenamoji vieta ar amžius, nors tikriausiai jiems didžiausią įtaką turėjo politinis išprusimas. Kiti tyrimai pateikia panašius rezultatus, tačiau taip pat pamini faktą, jog balsuojant internetu nebuvo galimybės matyti informacijos rusų kalba, kai rusai yra didžiausia mažuma Estijoje (apie 26 % populiacijos) [34].

3.1.5. Apibendrinimas

Apibendrinant Estijos elektroninio balsavimo schemą, bus atsižvelgta į privatumo ir verifikavimo aspektus. Rinkimai nuo 2013 metų gali būti laikomi anonimiškais, nes sukurama aplinka, kurioje išorinis asmuo negali nustatyti už ką balsavo rinkėjas naudodamasis vien tik viešai prieinama informacija ir laikant, kad rinkimų sistemos išorinis raktas yra saugiai perduodamas į balsavimo aplikaciją. Taip pat, pagal Smyth ir Bernhard, tai reiškia jog ši schema tenkina patvirtinimo nebuvimo sąlygą (angl. *receipt-freeness*). Naudojami šifravimo metodai nebūtinai užtikrina visiško privatumo. Jei rinkėjas gali įrodyti už ką jis balsavo, tai netenkina balsų patvirtinimo nebuvimo kriterijaus. Estijos rinkimų schema palaiko šią sąlygą, kadangi Estijos rinkimų sistemos taikomi verifikavimo mechanizmai taikomi kiekvienam balsui individualiai (ne tik paskutiniam), tačiau netenkinama atsparumo spaudimui sąlyga. Pavyzdžiui, rinkėjas gali atimti ar išreikalauti iš rinkėjo jo eID kortelę, atitinkamus PIN kodus ir popierinį balsavimo biuletenį. Tokiu atveju rinkėjas gali tiek gadinti, tiek kontroliuoti visus rinkėjo vardu atiduodamus balsus.

Taip pat sunkiai tenkinama korupcijos įrodymo sąlyga, kadangi balsai, atiduoti tradiciniu būdu, nėra lyginami su elektroniniu būdu atiduotais balsais, nei elektroniniai balsai yra lyginami tarpusavyje.

Kadangi Estijos balsavimo sistema nepateikia jokios bendros formos, kuri leistų peržiūrėti visus balsus, nėra tenkinama universalios verifikavimo sąlyga. Tai reiškia jog bet kuris rinkėjas negali patvirtinti, jog paskelbtas rinkimų rezultatas yra suma visų atiduotų balsų.

3.2. Prancūzijos elektroninio balsavimo sistema

Prancūzija pradėjo taikyti elektroninį balsavimą 2003 metais, kuris buvo skirtas prancūzams gyvenantiems už šalies ribų ir leista balsuoti prezidento bei aukštesniųjų rūmų rinkimuose.

2012 metais Prancūzijos emigrantai galėjo rinkti ir žemesniųjų rūmų atstovus elektroniniu būdu. Balsavimo aplikacija, kuri buvo naudota 2009 ir 2012 metais, buvo sukurta ispanų kompanijos „Scytll“. Rinkėjai, kurie norėjo balsuoti 2012 metų rinkimuose turėjo užsiregistruoti konsule ir jiems vėliau buvo atsiųstas prisijungimo ID paprastu paštu likus 15 dienų iki rinkimų. Likus 10 dienų iki rinkimų, ID buvo persiųstas SMS žinute. Prisijungimo slaptažodis buvo siunčiamas elektroniniu paštu likus 5 dienoms iki rinkimų. Pirmo ir antro rinkimų turo slaptažodžiai buvo skirtingi [35].

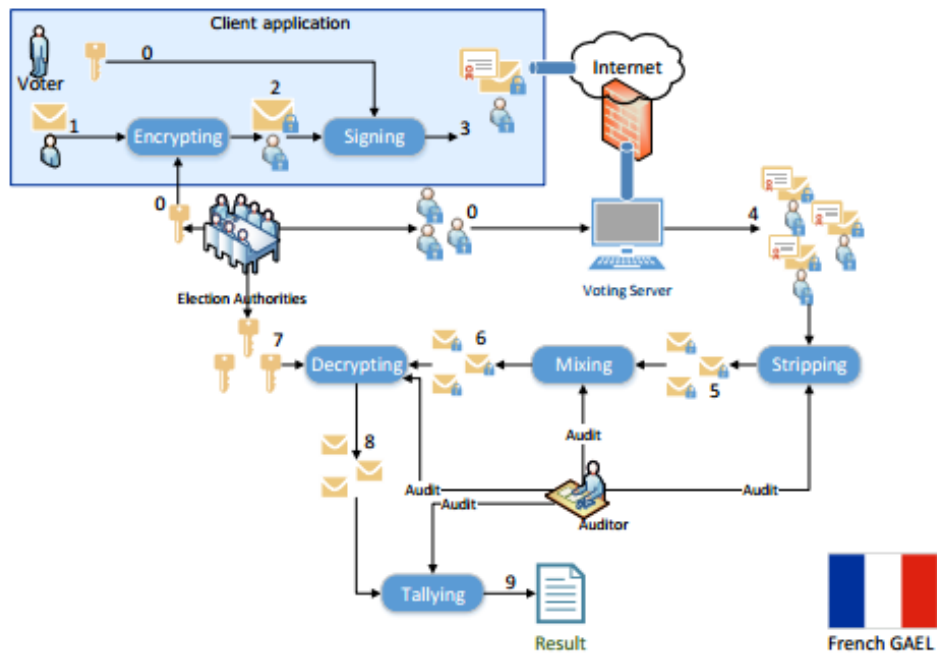
3.2.1. Prancūzijos elektroninio balsavimo schema

Prancūzijos elektroninio balsavimo schema nėra labai aiškiai dokumentuota, bet bendru atveju ji veikia taip:

Norint apsaugoti rinkėjo kompiuterį, elektroninio balsavimo tinklapis sugeneruoja saugią elektroninę balsavimo būdelę rinkėjo kompiuteryje. Kai rinkėjas atiduoda savo balsą, jis gauna balsavimo lapelį. Rinkėjas gali susikurti savo slaptažodį balsavimo aplikacijai, kam reikalingas jo valstybės išduotas identifikacinis numeris (NUMIC), vardas, gimimo data ir paso numeris [35].

Prancūzų balsavimo sistemą galima laikyti mažiausiai saugia žvelgiant iš rinkėjo autentikacijos pusės. Nors internetinė registracija reikalauja nemažai asmeninės informacijos, tačiau nors ir sudėtinga, tačiau įmanoma pašaliniams asmenims ją gauti. Tačiau reikia nepamiršti, jog Prancūzijos balsavimo sistema skirta skatinti emigravusių prancūzų dalyvavimą rinkimų procese, tad suprantama, jog sistemos prieinamumas gali būti aukštesnio prioriteto nei saugumas [35].

Tiek 2009, tiek 2012 metų rinkimuose, rinkėjo identifikacijai naudojamas NUMIC (valstybės išduotas identifikacinis numeris), kuris yra siunčiamas rinkimų organizatoriams kartu su užšifruotu ir pasirašytu balsu. Prieš iššifravimo fazę, nuo balsų yra atskiriamas NUMIC numeris. Kai baigiasi elektroninio balsavimo periodas, visi gautų rinkėjų NUMIC yra siunčiami į visus Prancūzijos konsulatus, kad tie rinkėjai nebegalėtų balsuoti kitais būdais.



2 pav. Supaprastinta Prancūzijos elektroninio balsavimo schema [27]

Žemiau pateikta autentikavimo procedūra, laikant jog rinkėjas jau parsisiuntė aplikaciją į savo kompiuterį bei aplikacija žino rinkimų organizatorių viešąjį raktą:

1. Rinkėjas aplikacijoje pasirenka norimą partiją ar kandidatą;
2. Rinkėjas užšifruoja savo NUMIC atskirai, naudodamasis viešuoju raktu;
3. Rinkėjas pasirašo savo užšifruotą balsą naudodamasis privačiu raktu. Užšifruotas bei pasirašytas balsas kartu su užšifruotu NUMIC yra siunčiamas į rinkimų serverį naudojant SSL protokolą;
4. Po internetinio balsavimo rinkimų periodo užšifruoti ir pasirašyti balsai, bei užšifruoti NUMIC yra siunčiami į apvalymo procedūrą, kuri atskiria užšifruotus NUMIC bei parašus nuo atiduotų balsų;
5. Patikrinama ar asmenys atidavę balsus turėjo teisę atiduoti balsą;
6. Balsai perduodami į iššifravimo procedūrą;
7. Iššifruoti balsai yra perduodami į apskaičiavimo procedūrą;
8. Apskaičiavimo procedūra pateikia galutinį elektroniniu būdu atiduotų balsų rezultatą [35].

Kiekvieną iš šių procedūrų atidžiai prižiūri atitinkamos srities nepriklausomi auditoriai.

3.2.2. Verifikacijos mechanizmas

2009 metų rinkimai buvo pirmieji, kuriuose prancūzai naudojo verifikacijos mechanizmą savo balsavimo sistemoje. Kaip ir su „ScytL“ sistema, rinkėjai gauna pranešimą savo kompiuteryje, kuris patvirtina, jog jų atiduotas balsas yra įskaitytas duotu laiku ir data. Galima šią žinutę peržiūrėti keletą kartų į rinkimų tinklapį įvedus rinkėjo kortelės numerį [34]. Šį verifikacijos būdą galima laikyti priėmimo verifikacija, kadangi nepateikiama informacija apie tai už ką buvo balsuota. Prancūzų emigrantai neturi galimybės perbalsuoti.

3.2.3. Statistika

Prancūzijos elektroninio balsavimo statistika yra paremta emigrantų balsais. 2003 metais 60.6 % visų atiduotų balsų buvo atiduoti elektroniniu būdu, 2006 skaičius krito iki 14 %, o 2009 iki 9 %, tačiau dėl sudėtingos rinkimų organizavimo gana sunku gauti tikslius skaičius. Priklausomai nuo rinkimų metų, skirtingi regionai, kuriuose gyvena emigrantai, turėjo teisę balsuoti. 2003 metais teisę balsuoti turėjo emigrantai gyvenantys Šiaurės Amerikoje, 2006 metais – Europoje, Azijoje ir vidurio rytuose, 2009 – Afrikoje bei Šiaurės ir Lotynų Amerikoje. 2003 metais rinkimai kainavo 61 000 Eurų, 2006 – 2 milijonus eurų. Kitų metų rinkimų kaina nėra tiksliai žinoma [34].

3.2.4. Apibendrinimas

Apibendrinant prancūzų elektroninio balsavimo schemą bus atsižvelgta į privatumo ir verifikacijos aspektus. Nuo 2009 metų vykstantys rinkimai tenkina balso privatumo sąlygą, kadangi išorinis asmuo neturi galimybės sužinoti už ką rinkėjas balsavo, naudojantis tik viešai prieinama informacija. Naudojamas šifravimo mechanizmas neužtikrina visiško balso anonimiškumo. Sistema taip pat nepalaiko balso patvirtinimo nebuvimo. Rinkėjui atiduodant balsą elektroniniu būdu galima filmuoti/fotografuoti jo kompiuterio ekraną, stebint už ką jis balsuoja. Kadangi nėra galimybės perbalsuoti, atiduotas balsas laikomas galutiniu.

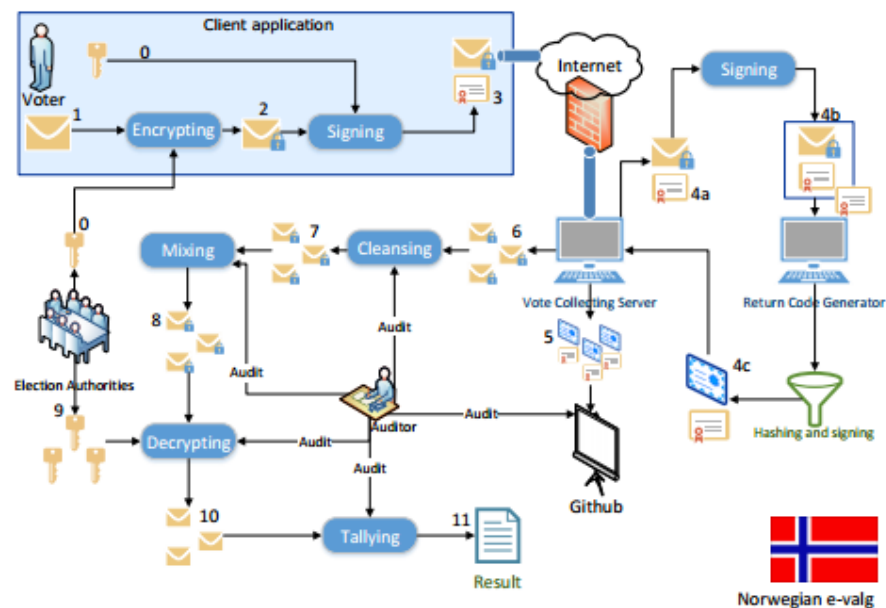
Prancūzijos balsavimo sistema taip pat nepalaiko universalios verifikacijos, t. y. bet kuris žmogus negali patvirtinti, jog paskeltas rinkimų rezultatas yra tiksli visų atiduotų balsų suma.

3.3. Norvegijos elektroninio balsavimo sistema

Norvegija palaikė elektroninį balsavimą 2011 metais kai kuriuose (10 iš 429) savivaldybių vietiniams rinkimams naudojami Ispanų kompanijos „Scytll“ sukurta sistema [34].

3.3.1. Norvegijos balsavimo sistemos schema

Norvegijos elektroninio balsavimo sistema autentikacijai naudoja elektroninę ID kortelę (mini ID) bei slaptažodį, kuris autentikuoja šią kortelę. Šis būdas naudojamas daugumoje Norvegijos valstybinių organizacijų. Mini ID leidžia rinkėjui prisijungti prie balsavimo tinklapio, kuris pateikia balsavimo aplikaciją, rinkėjo duomenis, įskaitant jo privatą pasirašymo raktą, išorinį rinkimų organizatorių raktą bei kandidatų ar partijų sąrašą.



3 pav. Supaprastinta Norvegijos elektroninio balsavimo schema [27]

Užkrovus aplikaciją pradedamas balsavimo procesas paaiškintas žemiau [34]:

1. Balsavimo aplikacija sukonfigūruota naudoti rinkimų organizatorių suteiktą išorinį raktą, rinkėjo privatų raktą bei turi užkrautą kandidatų sąrašą;
2. Rinkėjas pasirenka kam atiduos balsą;

3. Rinkėjas užšifruoja balsą naudodamasis rinkimų organizatorių suteiktu išoriniu raktu;
4. Rinkėjas pasirašo užšifruotą balsą savo privačiu raktu. Užšifruotas balsas perduodamas į balsų surinkimo serverį (angl. *Vote Collecting Server* – VCS) naudojant SSL protokolą;
5. Parašas bei atitinkamumas patikrinimas balsų surinkimo serveryje:
 - a) VCS dalinai iššifruoja gautą balsą;
 - b) VCS pasirašo užšifruotą ir pasirašytą balsą, kad įrodyti, jog sistema gavo balsą ir perduoda jį atgalinio kodo generatoriui (angl. *Return Code Generator* – RCG);
 - c) RCG apskaičiuoja užšifruoto balso hash funkciją ir pasirašo balsą prieš perduodant atgal VCS.
6. Kas valandą visi gauti nauji hash bei parašai iš RCG yra padedami į Github repositoriją. Kiekvienas balsas atitinka vieną eilutę Github faile. Tai įrodo jog RCG gavo ir apdorojo balsą;
7. Po rinkimų balsai yra atskiriami nuo parašų ir siunčiami į sutvarkymo procedūrą, kad sutvarkyti duomenis apie tiek elektroninius, tiek fizinius perbalsavimus;
8. Balsai tada yra perduodami į sumaišymo fazę, kur yra sumaišomi ir dar kartą užšifruojami;
9. Sumaišyti balsai yra perduodami iššifravimo fazei;
10. Politinės partijos suveda jiems paskirstytas skirtingas iššifravimo rakto dalis iš kurių pagaminamas galutinis iššifravimo raktas;
11. Iššifruoti balsai yra perduodami balsų skaičiavimo procedūrai;
12. Skaičiavimo procedūra pateikia galutinius rinkimų rezultatus;

Skirtingos sistemos dalys yra audituojamos nepriklausomo auditoriaus. Visi Github išsaugoti duomenys yra patikrinami su galutiniais rinkimų rezultatais.

3.3.2. Verifikacijos mechanizmas

RCG apskaičiuoja asmeninį rinkėjo kodą, kuris prieš tai buvo jam atsiųstas paprastu paštu. Nepaisant labai atidžios rinkimų sistemos priežiūros, išorinis auditorius tikrina ar skirtingos rinkimų fazės atliekamos korektiškai.

Įdomu tai, jog iki 2013 metų Norvegijos elektroninio balsavimo Sistema neviešino visų patiektų balsų (šiuo metu Github svetainėje), „siekiant užkirsti kelią balsų pirkimui“ [36].

Kaip ir Estijos sistema, Norvegijos sistema leidžia perbalsuoti įprastu būdu, kas anuliuos elektroninį balsą, tačiau Norvegijoje galima perbalsuoti ir rinkimų dieną. Per elektroninio balsavimo laikotarpį

galima perbalsuoti kiek tik norima kartų. Palyginti elektroninio balsavimo periodas yra gana ilgas – 30 dienų.

Dėl skaidrumo sumetimų, tiek visa rinkimų sistemos dokumentacija, tiek visas programos kodas yra viešai prieinamas visuomenei [34].

3.3.3. Statistika

2011 metų savivaldybių rinkimų balsavimo ataskaitoje iš 168 000 balsavimo teisę turinčių rinkėjų, 26,4 % balsavo internetu iš visų 104 374 atiduotų balsų. 2013 metų savivaldybių rinkimų balsavimo ataskaitoje iš 196 172 teisę turinčių rinkėjų, 36 % balsavo internetu iš visų 70 622 atiduotų balsų [34].

3.3.4. Apibendrinimas

Apibendrinant Norvegijos elektroninio balsavimo sistemą bus atsižvelgta į privatumo ir verifikacijos sąlygas. Rinkimai nuo 2011 metų tenkina balso slaptumo sąlygą, kadangi išorinis asmuo negali sužinoti už ką balsavo rinkėjas turint tik viešai prieinamą informaciją. Panašiai kaip ir kitų šalių sistemose, Norvegijos sistema nėra atspari tyčiniam rinkėjo duomenų atskleidimui, kai rinkėjas pats atiduoda savo identifikacinius duomenis, slaptažodžius ir k. t.

Nors Norvegijos ir skelbia visus atiduotus balsus, tačiau tai tėra jų hash funkcijų suma, kurios išoriniam asmeniui neatskleidžia jokios detalios informacijos nepaisant fakto, jog buvo balsuota. Dėl šios priežasties ši elektroninio balsavimo schema netenkina universalios verifikacijos sąlygos.

Kadangi ši sistema informuoja rinkėją jog jo balsas įskaitytas SMS žinute, bei yra galimybė perbalsuoti, galima laikyti, jog ši sistema yra pakankamai saugi. Jei rinkėjo duomenis būtų perėmęs išorinis asmuo, jam prabalsavus tikrasis rinkėjas gaus SMS žinutę apie ne jo atiduotą balsą. Ko pasekoje jis gali perbalsuoti (įskaitomas tik paskutinis balsas) arba kreiptis į atsakingas institucijas.

3.4. Elektroninių balsavimo sistemų analizė

Šiame skyrelyje bus apibendrintos Estijos, Prancūzijos bei Norvegijos elektroninio balsavimo sistemos. Patogumui, palyginimai bus pateikti lentelėje.

Estijos elektroninio balsavimo sistema laikoma tenkinanti balso slaptumo, balso nepriklausomumo, atsiskaitomybės nebuvimo sąlygas. Rinkėjai autentikuojami naudojantis dviejų lygių autentikavimo

metodus, naudojant tiek elektroninę ID kortelę (arba atitinkamą SIM), tiek PIN kodus. Pasibaigus išankstinio balsavimo periodui, rinkimų dieną nebeleidžiama perbalsuoti. Elektroninis balsavimas yra prieinamas visiems Estijos piliečiams nepriklausomai nuo to, ar jie gyvena užsienyje. Norint balsuoti internetu nereikalinga išankstinė registracija.

Prancūzų balsavimo sistemą galima laikyti tenkinančią balso slaptumo, balso nepriklausomumo sąlygas, tačiau netenkinama nei viena verifikavimo savybė. Rinkėjas gali užsiregistruoti pateikdamas valstybės išduotą unikalų numerį, vardą, gimimo datą bei paso numerį. Po to galima pasirinkti slaptažodį. Rinkėjo identifikavimas atliekamas tikrinant unikalų valstybės kodą bei pasirinktą slaptažodį. Rinkėjai išankstinio balsavimo metu gali balsuoti paštu arba elektroniniu būdu, arba rinkimų dieną ambasadoje, jei jie nebalsavo iš anksto. Elektroninis balsavimas yra prieinamas visiems balso teisę turintiems Prancūzijos piliečiams gyvenantiems užsienyje. Pakartotinis balsavimas nėra leidžiamas.

Norvegijos elektroninio balsavimo sistema laikoma tenkinanti balso slaptumo, balso nepriklausomumo, atskaitomumo nebuvimo sąlygas bei balso patvirtinimo verifikacijos aspektus. Rinkėjų registracija prieš elektroninį balsavimą nėra būtina. Rinkėjai identifikuojami taikant dviejų lygių autentifikaciją naudojant MiniID kortelę bei slaptažodį. Elektroninis balsavimas yra prieinamas balso teisę turintiems piliečiams iš atitinkamų savivaldybių tam tikrą laiką tarpą.

1 lentelė. Skirtingų šalių elektroninio balsavimo savybių palyginimas

Šalis	Balso slaptumas	Balso nepriklausomumas	Balso neatskaitomumas	Prievartai atspari	Universali verifikacija	Nereikia registracijos	Perbalsavimas e. balsavimu	Perbalsavimas įprastu balsavimu	Perbalsavimas rinkimų dieną
Estija	•	•	•			•	•	•	
Prancūzija	•	•							
Norvegija	•	•	•			•	•	•	•

Su konfidencialumu ir verifikavimu susijusių savybių palyginimas tarptautinėse elektroninio balsavimo schemose

2 lentelė. Skirtingų šalių elektroninio balsavimo identifikavimo būdų palyginimas

Šalis	Turi teisę balsuoti	Identifikavimo būdas
Estija	Visi piliečiai	Dviejų lygių: eID (arba SIM) ir atitinkami PIN kodai
Prancūzija	Visi užsienyje gyvenantys piliečiai	Vieno lygio: Įvedant unikalų valstybės išduotą kodą, vardą, gimimo datą, ir paso numerį
Norvegija	Piliečiai iš atitinkamų savivaldybių	Dviejų lygių: MiniID kortelė ir atitinkamas slaptažodis

4. Saugumo tikrinimo modelis

Šiame skyriuje bus aprašytas siūlomas modelis, kaip suskaidyti bei įvertinti kenkėjo žalą, kurią jis gali padaryti norėdamas pakenkti rinkimų procesui bei įvertinti pastangas, kurių reikia norint sėkmingai atakuoti rinkimų sistemą. Kenkėjo pastangos pagrindu susideda iš dviejų dalių – laiko ir finansinių išteklių. Laiko sąnaudos gali būti aktyvios (kenkėjas kažką daro) arba pasyvios (laukiant kol kažkas kitas kažką padarys). Laiką galima skaidyti į „prieš balsavimo periodą“ bei „rinkimų periodo metu“. Šiame skyriuje bus pabrėžta, kodėl svarbu laiką skaidyti į šias dalis. Finansiniai ištekliai gali būti fiksuoti arba kintantys, nuo ko priklauso kenkėjo tikslas. Siūlomo modelio tikslas yra ne tik suskaidyti ir išanalizuoti galimas atakas, tačiau ir palyginti įvairių atakų įtaką remiantis sutartu atskaitos tašku bei atrasti galimus atakų prevencijos būdus.

4.1. Aktoriai (veikėjai)

Atakos metu gali dalyvauti keletas aktorių. Šiame poskyryje bus pateiktas neformalus šių aktorių modelis. Galima išskirti penkis aktorius: kenkėjai, rinkėjai, rinkimų organizatoriai, IT asmenys bei auditoriai.

4.1.1. Kenkėjai

Pagal Storer ir Duncan [37] atliktą tyrimą, nustatyti trys galimi kenkėjų tipai:

- 1) Kenkėjiški rinkimų organizatoriai, siekiantys arba nepripažinti tam tikrų rinkėjų balsų, arba stebėdami už ką balsuoja atitinkami asmenys. Toks kenkėjas gali būti tapatinamas su priespauda taikančiu režimu ar valdžia, siekiant destabilizuoti demokratinį procesą;
- 2) Kenkėjiškas rinkėjas, turintis balsavimo teisę bei siekiantis sutrikdyti demokratinį procesą;
- 3) Išorinis kenkėjas, siekiantis sutrikdyti demokratinį procesą. Jie identifikuojami kaip užsienio agentai, šnipai, kriminalinės organizacijos protesto grupės ar tyrinėjantys žurnalistai.

Verta pažymėti, jog pirmame punkte paminėtos rinkimų organizacijos taip pat gali tyčia keisti balsus. Skirtingi kenkėjai gali turėti skirtingus tikslus, resursus bei finansus, kad įgyvendintų savo ataką. Taip pat, kai kurios atakos siekia būti nepastebėtos auditavimo mechanizmų, kai kitos kaip tik siekia būti pastebėtos, kad sukeltų nepasitikėjimą elektroninio balsavimo sistema. Kad nustatyti kokias atakas gali įvykdyti kenkėjas, būtina nustatyti kiekvieno kenkėjo galimybes, arba sukurti/suprasti kenkėjo modelį.

4.1.2. Rinkėjai

Laikoma, jog rinkėjai elektroninio balsavimo schemose naudoja savo kompiuterius (arba panašius įrenginius, kaip išmanieji telefonai ar planšetės) namuose, darbe arba kitur, kad atiduotų savo balsą. Trechsel ir Vassil [39] atliktas tyrimas pateikia duomenis apie Estijos elektroninių balsų atidavimą balsuojant iš namų skaičiaus mažėjimą, lyginant 2005, 2007 ir 2009 metų rinkimus. Tai galima iš dallies paaiškinti dėl to, jog Estijoje sparčiai daugėjo asmenų, kurie turi interneto prieigą namuose, skaičius. Šiame darbe kiekvienas rinkėjas bus laikomas kaip rinkėjas, kuris balsuoja internetu ir tai atlieka iš namų ar darbo/mokslo įstaigos. Estijoje, 76,6 % internetu balsavusių rinkėjų 2009 metų rinkimuose balsavo iš namų, o 21,7 % iš darbo ar mokymosi įstaigos. Paprastumo dėlei šie skaičiai bus suapvalinti iki 80% balsavusių iš namų ir 20% iš darbo ar mokslo įstaigos. Jų įrenginiai gali būti užkrėsti kenkėjiška programine įranga arba jų ryšio kanalas su internetu gali būti valdomas kenkėjo. Paprastumo dėlei bus laikoma, jog naudojama kenkėjiška programinė įranga tinka visiems rinkėjo naudojamiems įrenginiams.

4.1.3. Rinkimų organizatoriai

Rinkimų organizatoriai yra modeliuojami kaip piliečiai, kur įmanoma papirkti ar įtakoja daugiausia tik vieną iš jų. Tai reiškia, jog, pvz. skirstant iššifravimo rakto dalis, kenkėjas gali gauti daugiausiai tik vieną iš šio rakto dalių. Taip pat tai reiškia, jog daugiausiai vienas rinkimų organizacijos narys gali būti papirktas, kad pakeistų duomenis rinkimų sistemoje arba pažeistų konfidencialumo sąlygas.

4.1.4. Su IT susiję asmenys

IT asmenys, kurie atsakingi už sistemos implementaciją, testavimą bei priežiūrą modelyje užima labai svarbią vietą, kadangi jie turi tiek žinias, tiek prieigą prie atitinkamų sistemos dalių, kurios laikomos saugios ar konfidencialios. Modeliuojant ataką, gali būti, jog reiks pasinaudoti vienu iš šių asmenų, kad sėkmingai ją įgyvendinti. Kaip ir su rinkimų organizatoriais, IT asmenys bus laikomi atsparūs papirkimui ir jog ne daugiau, kaip vienas asmuo gali būti papirktas ar jo prisijungimo duomenys pavogti.

4.1.5. Auditoriai

Kaip minėta 3 skyriuje, visos nagrinėtos schemas, kurios naudojamos rinkimų sistemose turi išorinius stebėtojus, dažniausiai vadinamus auditoriais. Siūlomame modelyje auditorius turi specialią rolę kaip atitinkamų sistemos veikimo procesų tikrintojas. Auditoriaus darbą apima tokios atsakomybės, kaip tikrinimą, kas turi fizinę prieigą prie svarbių serverių, kas gali prisijungti prie jų iš išorės, viešojo bei privataus rakto tikrinimą ir kita.

4.1.6. Kyšininkavimas ir papirkinėjimas

Kaip buvo teigta anksčiau, šiame modelyje bus laikoma, jog yra neįmanoma papirkti daugiau nei vieno asmens iš rinkimų organizatorių, IT asmenų ar auditorių. Pasirenkant šią sąlygą buvo remtasi tuo, jog papirkinėjant daugiau nei vieną asmenį, smarkiai didėja tikimybė įkliūti. Tai nereiškia, jog neįmanoma papirkti daugiau nei vieną asmenį, tačiau remiamasi, jei kiekvieną rinkimų procesą prižiūri daugiau nei vienas asmuo, jį galima laikyti saugiu. Esant didesniam atsakingų žmonių skaičiui, didesnė tikimybė, jog sąžiningi darbuotojai pastebės kenkėjiškus sistemos pakeitimus arba netinkamą kolegų elgesį.

4.2. Kenkėjo modelis

Kaip buvo minėta ankstesniame poskyryje, buvo įvesti keli apribojimai kyšininkavimo ir papirkinėjimo atveju. Nepaisant šių apribojimų, kenkėjas, planuodamas ataką, turi įvertinti ir kitus faktorius. Bendram modeliui bus sukurtas kenkėjo modelis, kuris daugiausia paremtas Dolev ir Yao grėsmių modeliu [40]: kenkėjas turi pilną prieigą prie tinklo bei gali matyti, analizuoti, pakartoti, išmesti bei keisti kiekvieną apsiųstą pranešimą, taip pat gali pridėti ir naujus pranešimus. Sudarant kenkėjo modelį bus laikomasi, jog jis gali daryti ką tik nori, išsikrus šiuos dalykus:

- 1) „Nulaužti“ ne trivialius užkoduotus pranešimus, tačiau gali tai padaryti naudodamas „brute force“ metodą, kai iš turimo žodyno bandomos visos galimos dešifravimo kodo kombinacijos;
- 2) „Nulaužti“ saugius ryšio kanalus tarp skirtingų sistemos modulių;
- 3) „Nulaužti“ oro ryšio kanalus;
- 4) Gauti visą arba dalį iššifravimo raktų iš rinkimų organizatorių;
- 5) Apeiti auditoriaus atliekamus patikrinimus;
- 6) Papirkti daugiau nei vieną narį iš rinkimų organizatorių, IT asmenų ar auditorių;
- 7) Gauti konfidencialią informaciją ar apeiti PIN apsaugotas išmanias korteles;
- 8) „Nulaužti“ apsaugotą ne vartotojo lygmens komponentą (pvz. serverį) ir pakeisti, ištrinti ar pridėti informacijos ar programinės įrangos.

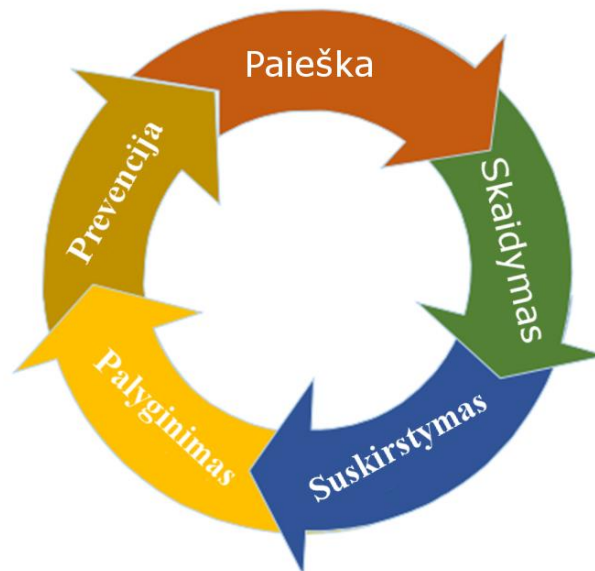
4.2.1. Kenkėjo modelio pritaikymas

Toliau aptariamos galimos atakos bus suskaidytos ir įvertintos pagal jų kainą bei laiką, kurį reikia sugaišti kenkėjui, kad sėkmingai įgyvendintų ataką. Priklausomai nuo kenkėjo įgūdžių, kenkėjų skaičiaus, turimo užkrėsto tinklo (angl. *botnet*) ir kt. kainos ir laiko sąnaudos gali būti padidintos ar sumažintos. Apskaičiuojant sąnaudas bus remiamasi turimais duomenimis, kuriuos reikalui esant galima pakeisti kitų šalių informacija.

4.3. Modelis

Šiame poskyryje bus aptartas siūlomas modelis bei paaiškinti jame vyraujantys žingsniai bei sprendimai.

Kad būtų įmanoma iš anksto nustatyti visas įmanomas atakas, suskaidyti jas į dedamąsias pagal pastangas, kurias turi įdėti kenkėjas, jas suskirstyti bei palyginti reikia apsirašyti tikrinimo modelį. Siūlomame modelyje reikalingi žingsniai atliekami eilės tvarka bei gali būti pradėti iš naujo. Po atakų aptikimo ir jų išvengimo ar prevencijos sprendimų priėmimo galima iš naujo atlikti paieškos, skaidymo, suskirstymo, palyginimo bei prevencijos žingsnius, kad toliau tobulinti turimą elektroninio balsavimo schemą. Šis procesas pateiktas 4 pav.



4 pav. Siūlomo saugumo tikrinimo modelio principinė schema [40]

4.3.1. Paieška

Nepaisant to, kad net ir paprastame IT projekte yra gana sudėtinga išaiškinti visas įmanomas rizikas, elektroninio balsavimo projektas yra sudėtingas ir nuo daug ko priklauso. Elektroninio balsavimo projektai priklauso ir yra vystomi aplink tiek IT infrastruktūrą, tiek ir žmogiškųjų išteklių reguliavimą. Weldemariam ir Villafiorita [41] tai aprašė kurdami metodologiją, kad galėtų atlikti procedūrinę saugumo analizę. Jie sumodeliavo būdą, kad galėtų formaliai aprašyti įvykių (veiksmų) eigą, kurios pereina įvairios esybės (pvz. balsai, rezultatai ir k. t.), kurios ribojamos procedūrų (pvz. auditoriaus

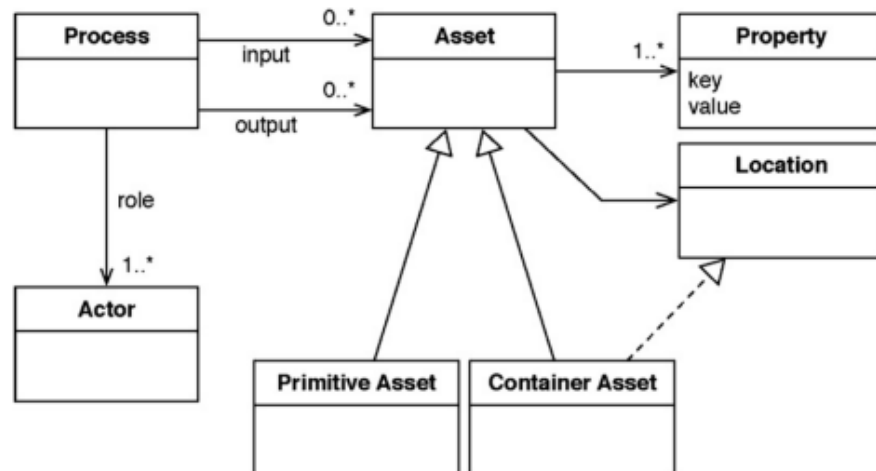
patikrinimai ar balsų valymas). Jų tikslas yra identifikuoti įvairias galimas atakas taikant automatizuotus sprendimus, ko pasėkoje galima atlikti išsamią atakų paiešką.

4.3.1.1. Paieškos esminis principas

Pagal Weldemariam ir Villafiorita [41] pateiktą metodą, pirma aprašoma kiekviena esybė (pvz. rinkimų biuletenis, balsas, programinės įrangos dalis) su jos atributais ir jos susiejamos su atitinkamomis procedūromis. Esybių atributai gali būti laisvai pasirenkami ir vėliau naudojami sudarant grėsmių modelį. Atributai, kaip pavyzdys, gali būti „užšifruotas“, „pasirašytas“ ir kt. Jie taip pat gali atitikti fizinės daiktų būsenas, kaip „uždarytas“ seifas, „užplombuota“ balsadėžė, arba būti iš anksto nustatyti, kaip „lokacija“, „turinys“ ir kiti.

Kiekvieną esybę gali turėti daug egzempliorių (pvz. rinkimų biuletenių). Kiekviena esybė gali būti arba primityvi, arba talpinančioji (angl. *container*). Talpinančiosios esybės gali savyje turėti arba kitą talpinančią esybę arba primityvią esybę (pvz. balsadėžė turi rinkimų biuletenius).

Procesai kuria, pašalina arba keičia esybių atributus (pvz. pasirašymo procesas pakeičia atiduodamo balso esybės savybę „pasirašytas“ į „Taip“). Kiekvienu laiko momentu kiekviena esybė turi atitinkamą būseną (pagal jų atributus). Atributai yra keičiami proceso dėka, kuriuos galima stebėti ir tikrinti ar jie vyksta sklandžiai. Kiekvienas iš procesų turi 1 ar daugiau aktorių, kurie gali jį valdyti. 5 pav. pateikta diagrama, kurioje pavaizduota, kas buvo aptarta.



5 pav. Procedūrinio saugumo analizės metodologinio principo esybių diagrama [41]

Pagal Weldemariam ir Villafiorita [41], šio aprašymo pakanka, kad būtų galima sumodeliuoti paprastas atakas ties viena esybe, kadangi yra žinomas esybės turinys, jos lokacija, tad galima nesudėtingai nustatyti kaip galima pakeisti šių esybių būseną „kenkėjišku“ būdu. Tačiau autoriai taip pat pabrėžia, jog šio aprašymo nepakanka, kad aprašyti sudėtingas atakas, kuriose ataka gali būti nukreipta prieš grupę esybių vienu metu. Šiuo atveju yra siūloma kenkėjus modeliuoti kaip aktorius, kurie gali valdyti naujus kenkėjiškus procesus arba naudoti jau esamus procesus, kurie pakeičia esybių būseną į ne iš anksto nustatytą.

Šie kenkėjiški procesai gali būti sudaryti iš paprastų šalinimo, skaitymo, atnaujinimo ar kūrimo procesų, pvz. perrašymo kenkėjiškas procesas susideda iš kelių paprastų procesų: originali esybė buvo pašalinta ir nauja buvo sukurta, tad pakeitimo procesas susideda iš dviejų įvesties ir vienos išvesties esybių. Paprastai tariant, jei kiekvienai esybei modeliuotume procesus su visais paprastaisiais procesais (CRUD – angl. *Create, read, update, delete*), gautume visas galimas grėsmes ties kiekviena esybe.

4.3.1.2. NuSMV

Weldemariam ir Villafiorita [41] siūlo būdą, kaip modeliuoti tiek įvykių seką (angl. *workflow*), tiek kenksmingus procesus naudojant simbolinę modelių (angl. *symbolic model*) tikrinimo kalbą NuSMV.

Pagal jų siūlomą metodologiją, jie pirma aprašo įprastinę įvykių seką (angl. *workflow*), aprašant esybes ir procesus NuSMV kalba ir duoda atitinkamos srities specialistams išanalizuoti ir nustatyti esybių atributus bei procesų detales. Jie modeliuoja esybes, kaip turinčias ribotą kiekį galimų būsenų (angl. *finite state-machines*), kurios gali keisti būseną, kai tenkinamos iš anksto nustatytos sąlygos. Šioje pradinėje stadijoje nėra įtraukta kenkėjo galimos įtakos analizė. Veiksmų seka (angl. *workflow*) yra modeliuojama turint „programinį skaitiklį“ (angl. *program counter*), kuris nusprendžia, kuris procesas bus sekantis bei kokios esybės jame dalyvauja, bei tikrinant ar visos išankstinės sąlygos yra tenkinamos. Veiksmų sekos (angl. *workflow*) bei ribotų būsenų esybių sąjunga tarpusavyje vieną kitą įtakoja bei keičia. Pagal šią sąjungą galima išplėsti turimą modelį (randant galimas silpnąsias vietas) ir sukurti naują modelį, kuriame įtrauktas ir kenkėjas.

Abu modeliai yra aprašyti NuSMV kalba. Kiekviena esybė aprašyta, kaip turinti ribotą skaičių galimų būsenų su atitinkamomis išankstinėmis sąlygomis, kurios gali būti gautos iš esybės atributų, aktorių bei programinio skaitiklio veiksmų sekoje (angl. *workflow*). Kylančių grėsmių (angl. *threat-action*) modelyje, kuriame yra įtrauktas ir kenkėjas, turi papildomus kintamuosius, kurie galima matyti kas vyksta (pvz. kad balsavimo aplikacija yra netikra). Tipinis NuSVM verifikavimas naudojantis

atitinkamus įrankius išves visas silpnąsias vietas atakoms įvykti. Tai leidžia pamatyti, kaip ataka gali būti vykdoma ir atitinkamai imtis apsauginių priemonių.

4.3.1.3. Atakų paieškos modelio pagrindimas

Šiame skyriuje aptartas Weldermariam ir Villarfiorita pasiūlytas būdas, kaip aptikti atakas turint apsirašytą modelį. Jų pasiūlytas būdas leidžia ne tik formaliai atvaizduoti galimas grėsmes, bet ir padeda lengviau suprasti, kaip veikia sistema, pateikiant gana detalią informaciją apie kiekvieną esybę bei vykdomus procesus. Atitinkamos srities specialistų pateikta informacija yra formalizuojama ir aprašoma, sudarant aiškias ir paprastas nagrinėti diagramas (veiksmų diagrama, aktorių diagrama ir t.t.), kas leidžia lengviau aptikti papildomas grėsmes ar pasiūlyti patobulinimų.

Šio sprendimo stiprioji pusė yra ne tik aptikti, kiek įmanoma daugiau grėsmių, tačiau ir dokumentuoti sistemos veikimą.

Norint sėkmingai naudoti šį būdą, reikia atlikti sekančius žingsnius:

1. Aprašyti visas esybes bei jų atributus remiantis ar konsultuojantis su atitinkamos srities specialistais;
2. Nustatyti procesus bei aktorius, kurie sąveikaus su esybėmis;
3. Sudaryti veiksmų seką (angl. *workflow*), bei ją suprogramuoti naudojant NuSMV;
4. Aptikti bei įvertinti rastas grėsmes (atakas).

4.3.2. Skaidymas

Nustačius galimas atakas naudojant prieš tai aptartą metodą, galima kiekvieną iš jų išskaidyti (angl. *quantify*). Kaip minėta anksčiau, skaidymas paremtas kenkėjo patiriamomis sąnaudomis, kurias jis turi patirti, kad įvykdytų ataką. Laiko sąnaudos bus išreikštos aktyviu ir pasyviu laiku dienomis, prieš ir per rinkimų laikotarpį, o finansinės sąnaudos bus išreikštos fiksuotomis bei kintančiomis kainomis.

Norint tai įgyvendinti, reikia skaidyti kiekvieną aptiktą ataką, kuri buvo rasta siūlomo modelio paieškos fazėje.

4.3.2.1. Atakų medžiai

Pasiūlytas būdas 4.3.1 skyriuje leidžia rasti galimas atakas, iš ko galima nustatyti kaip esybės yra manipuliuojamos norint įvykdyti ataką. Šios manipuliacijos gali būti suskirstytos į dvi kategorijas:

- Aktoriai elgiasi ne taip kaip turėtų;
- Procesai atlieką ne tą ką turėtų (tiek kenkėjo sukurti, tiek netinkamai naudojami iš anksto sukurti).

Atakų medžiai leidžia detalai nagrinėti skirtingas atakos dalis. Kiekviena iš atitinkamų esybių manipuliacijų gali būti pastebėta rinkėjų, kandidatų, IT žmonių, rinkimų organizatorių, auditorių ar kitų žmonių. Svarbu tai įvertinti, jei vienas iš kenkėjo tikslų yra, jog ataka liktų nepastebėta.

Jei atakai reikalinga, jog kažkuris aktorius elgtųsi ne taip, kaip turėtų, reikia juos „paskatinti“, jog jie taip elgtųsi. Tai galima pasiekti keliais būdais, dažniausiai paperkant ar priverčiant. Kaip minėta anksčiau, laikomasi, jog neįmanoma paveikti daugiau nei vieno aktoriaus, tačiau reikalui esant galima šią sąlyga koreguoti.

Jei atakai reikalinga manipuluoti esybėmis naudojant procesus ne pagal paskirtį, nėra iškart aišku, kaip tai reiktų pateikti atakos medyje. Prieš tai aptiktoje atakoje nėra pateikta, kokius specifinius žingsnius reikia atlikti atakai įgyvendinti. Kadangi IT personalas jau buvo prieš tai įtrauktas nustatinėjant galimas atakas, juos taip pat reiktų įtraukti ir į atakų medžio sudarymo veiklą.

Svarbu įvertinti lokaciją, kurioje ataka yra galima. Pavyzdžiui, yra neįmanoma pasirašyti suklastoto balso serverio pusėje, jei nei serveris, nei kenkėjas neturi atitinkamo vartotojo pasirašymo rakto. Dėl šios priežastis kenkėjas tai turėtų atlikti ten, kur įmanoma raktą nusikopijuoti arba pakeisti pasirašymo procesą, kuris praleistų suklastotą balsą.

Fizinės bei skaitmeninės lokacijos gali būti suskirstytos į tris dalis:

1. Klientinė dalis. Pvz., balsavimo aplikacija, mobilusis telefonas;
2. Serverio dalis. Pvz., patys serveriai, vidinis tinklas ar auditoriaus aplinkos;
3. Sujungimai tarp šių lokacijų, kaip internetas ar telefoninės linijos.

Atakos, kurios vyksta klientinėje dalyje, reikalauja, jog kenkėjas manipuluotų esybėmis, kurios yra kliento balsavimo medijose (kompiuteris, telefonas ar kitas įrenginys, kuris yra prijungtas prie interneto) arba jo verifikavimo medijose. Tai galima įgyvendinti arba rankiniu būdu įsilaužiant į atitinkamą mediją, arba paskleisti kenkėjišką programinę įrangą į jau „nulaužtus“ kompiuterius. Kadangi, tikėtina, jog tokio

tipo atakos bus įgyvendinamos gana plačiu mastu, labai tikėtina, jog bus naudojamosi „mokėk už instaliaciją” (angl. *pay-per-intall* – *PPI*) paslauga, kad paskleisti kenkėjišką kodą jau į iš anksto nulaužtus kompiuterius.

Priklausomai nuo atakos tipo, gali tecti įsiterpti (angl. *inject*) į rinkėjo kompiuteryje veikiančią balsavimo aplikaciją / tinklapį arba tik pasyviai stebėti ekraną ar srautą tinkle. Kai kurioms atakoms reikia turėti „Command and Control” (toliau – C&C) infrastruktūrą, iš kurios galima siųsti komandas kenkėjiškai sistemai valdyti.

Ne visoms atakos, kaip ataka, kuri pašalina visus balsus, reikalinga tokia infrastruktūra. Tipiniu atveju įdiegiant kenkėjišką programą į rinkėjo kompiuterį, naudojamą elektroniniam balsavimui per rinkimų laikotarpį bus einama šiuo keliu:

- Galimai reikės pirkti C&C infrastruktūrą;
- Galimai gali tecti sukurti C&C infrastruktūrą;
- Parašyti programą, kuri manipuluos esybes;
- Pirkti kompiuterius naudojant PPI paslaugą;
- Paskirstyti talpyklos kenkėjišką kodą (angl. *placeholder*) – trumpai tariant, paruošti nupirktą kompiuterį ateityje diegiamai kenkėjiškai programai;
- Galimai dekompiliuoti balsavimo aplikaciją;
- Sukurti netikrą balsavimo aplikaciją / kenkėjišką programą;
- Paskirstyti kenkėjišką programą į talpyklas nupirktuose kompiuteriuose;
- Paleisti kenkėjišką programą rinkėjo kompiuteryje.

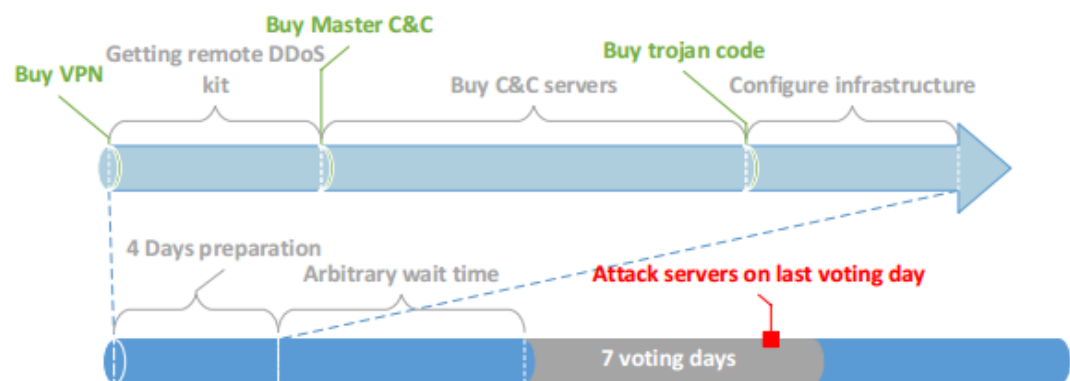
Norint įgyvendinti atakas serverio pusėje, kenkėjui reikia pačiam įsilaužti į serverius. Laikantis sąlygos, jog serveriai yra naudojami tik elektroniniam balsavimui, jie gali būti stebimi (angl. *monitor*) labai efektyviai. Bet koks mėginimas įsilaužti, pradedant nuo veikiančių servisų portų (angl. *port*) skanavimo gali būti lengvai pastebimas.

Atakos, kuriose manipuluojama esybėmis tarp kliento ir serverio lokacijų, kenkėjas veikia kaip tarpininkas. Nors didžioji dalis srauto, keliaujančio internetu yra užšifruota, dėl to mažai tikėtina, jog pavyks įgyvendinti klasikinę „Man in the middle“ ataką.

4.3.2.2. Dienos

Šiame poskyryje bus aptarta, kaip papildyti atakos medžius konkrečia informacija – dienų skaičiumi, kurį turi sugaišti kenkėjas, kad įgyvendintų ataką. Nustatę dienų skaičių kiekvienam atakos elementui galėsime paskaičiuoti galimą atakos kainą (kainos už tam tikras paslaugas yra žinomos). Kuo ilgiau reikia ruoštis atakai, tuo mažiau tikėtina, jog ji bus sėkmingai įgyvendinta.

Visų pirma, reiktų sudaryti laiko grafiką (6 pav.), kad būtų galima vizualiai matyti sąsajas ir sąnaudas tarp skirtingų atakos komponentų.



6 pav. Laiko grafiko pavyzdys [38]

Kiekvienas iš pateiktų žingsnių gali būti papildytas konkrečia laiko informacija pagal 3 lentelėje pateiktus duomenis. Lentelėje atskirai pateiktas tiek pasyvus, tiek aktyvus laikas, kurį reikia sugaišti.

Laikoma, kad aplikaciją galima dekompiliuoti per 4 – 5 dienas, kartu ir sukuriant netikrą jos versiją, tačiau užtektų tik 2 dienų, kad dekompiliuoti aplikaciją ir sukurti paprastą konfidencialios informacijos surinkimo įrankį.

3 lentelė. Laiko sąnaudos kenkėjo modeliui [38]

Užduotis	Iš anksto ar per laikotarpį	Aktyvios laiko sąnaudos (dienomis)	Pasyvios laiko sąnaudos (dienomis)
Dekompiliuoti balsavimo aplikaciją ir sukurti netikrą	Per laikotarpį	4 - 5	0
Dekompiliuoti balsavimo aplikaciją ir įterpti šnipinėjimo programą	Per laikotarpį	2	0
Nusipirkti 30000 PPI vienoje šalyje	Iš anksto	0	1
Paskleisti kenkėjišką programą į „talpyklą“	Per laikotarpį	0	1
Užkrėsto tinklo (angl. <i>botnet</i>) konsultacija	Iš anksto	1	0
Patobulinti standartinį botnet valdymą	Iš anksto	2	0

4.3.2.3. PPI

Ne visoms atakoms reikia PPI (angl. *pay-per-install*) paslaugos, bet toms kurioms reikia, reiktų įvertinti tikslų skaičių pirkimui, kad būtų galima nustatyti kainą. Visų pirma reikia žinoti „aukų“ skaičių (pvz. skaičius balsų, kuriuos reikia pakeisti, kad laimėti vieną vietą Seime, DDoS atakos stiprumas ir t.t.). Kad gautume šiuos skaičius, reikia išnagrinėti įvairią statistiką, pvz. visų turimų kompiuterių šalyje skaičius, skaičius registruotų elektroninių rinkėjų, procentas kompiuterių, kurie naudojami elektroniniam balsavimui, likęs elektroninių balsuotojų skaičius po pasiruošimo atakai.

Ypatingai svarbu įvertinti paskutinį dėmenį (e. balsuotojų skaičius po pasiruošimo atakai). Kaip pavyzdį galime laikyti, kad ataka bus ruošama 5 dienas iš 7 dienų balsavimo internetu laikotarpio. Galimas dar nebalsavusių rinkėjų skaičius, tikėtina, bus ženkliai mažesnis.

Taip pat, reikia įvertinti faktą, jog kiekvienas nupirkta kompiuteris naudojant PPI paslaugą turi tam tikrą sėkmės (ar nesėkmės) tikimybę, siekiant įdiegti kenkėjišką kodą, jog kompiuteris bus įjungtas

rinkimų periodo metu ir kad išvis kompiuteris bus naudojamas elektroniniam balsavimui paskutinėmis rinkimų periodo dienomis. Vien tai įvertinus, reikiamų PPI skaičius gali didėti bent 10 kartų, negu lyginant su iš anksto nustatytu reikiamu jų skaičiumi.

Verta paminėti, jog kai kurie paruošiamieji darbai gali būti atlikti prieš rinkimų laikotarpį, jei būtų nuspręsta anksčiau pavišinti balsavimo aplikaciją.

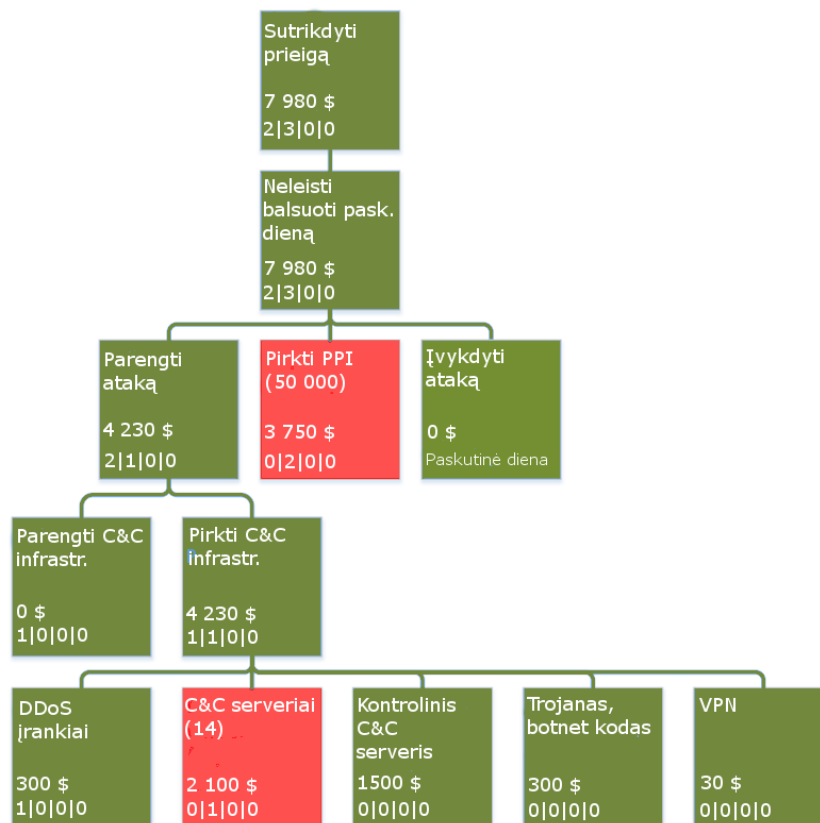
4.3.2.4. Kaina

Šiame poskyryje atakos medis bus papildytas informacija, įskaitant kainą. Kainas reikia suskirstyti į pastovias bei kintančias, kas leidžia parašyti funkciją, iš kurios pagal turimus duomenis galima gauti atakos kainą.

Kai kurie atakos žingsniai turi būti įvykdyti preciziškai, tačiau skaitmeninė šešėlinė rinka siūlo konsultacines paslaugas skirtingiems atakų tipams. Taip pat tikėtina, jog kenkėjas norės likti nepastebėtas. Skaitmeninė šešėlinė rinka taip pat siūlo sprendimus šiai problemai, kaip proxy ar virtualaus privataus tinklo (angl. *virtual private network* – toliau VPN) serveriai.

Norint paruošti C&C (angl. *Command-and-control*) infrastruktūrą, reikia kruopščiai įvertinti maksimalias vieno serverio valdymo galimybes. Laikoma, kad apie 600 kompiuterių gali būti valdomi vieno serverio. Šių serverių klasteris gali būti kontroliuojamas motininio C&C serverio, kuris tik komunikuoja su kitais serveriais ir yra apsaugotas nuo DDoS atakų, kad užtikrinti, jog jam nebus trukdoma veikti.

Įvertinus įvairius aspektus bei detales sudarant atakos medį ir turint preliminarų „aukų“ skaičių, įvairūs žingsniai atakos medyje gali būti papildyti detalesne informacija. 7 pav. pateiktas atakos medžio pavyzdys. Kainos pateiktos kiekviename mazge, kartu su laiko sąnaudomis (aktyvios išankstinės | pasyvios išankstinės | aktyvios per periodą | pasyvios per periodą). Raudoni mazgai yra kintančios išlaidos, žalios yra fiksuotos.



7 pav. Detalaus atakos medžio pavyzdys

Naudojant papildytą atakos medį galima sudaryti kainos funkciją, kuri susidės iš skirtingų atakos komponentų laiko bei kainos sandaugos sumos.

4.3.2.5. Suskirstymas

Šio žingsnio tikslas yra sugrupuoti atakas pagal užduotus požymius, jas nustatyti, bei įvertinti galimą įtaką rinkimų procesui. Atakas galima skirstyti į kategorijas, kurias siekiama sukompromituoti:

- Skaidrumas – siekiama sukelti abejonių, jog rinkimų sistema veikia skaidriai. Pvz. skleidžiant žinias, jog sistema yra nesaugi;
- Patvirtinimas – atakos, kuriomis siekiama paveikti/sutrikdyti patvirtinimo mechanizmą. Pvz. siunčiant netikras SMS žinutes rinkėjui, po to, kai jis balsavo;
- Sąžiningumas – Atakos, kurios keičia balsus, kad įtakotų rinkimų rezultatus;

- Laisvas pasirinkimas – Atakos, kurios riboja rinkėjo pasirinkimo laisvę, pvz. pašalinant kandidatus iš kandidatų sąrašo ar pavišinant išankstinius rezultatus, kad šie įtakotų jo pasirinkimą;
- Prieinamumas – Atakos, kurios rinkėjui riboja prieigą prie elektroninio balsavimo sistemos (DDoS ataka).

4.3.2.6. Palyginimas

Suskaidžius ir suskirsčius atakas galima pas palyginti. Galima jas lyginti tiek imituojant atakas prieš skirtingas elektroninio balsavimo schemas, tiek pagal jų grupę, tačiau šiame darbe labiausiai akcentuojami atakos įgyvendinimo kaštai bei pasekmės.

Jei turime nustatę ribinę atakos padarinio vertę arba atakos kainą, galime prioretizuoti, kuriai atakai reikia pirma užkirsti kelią. Pvz. jei ataka yra žemiau nubrėžtos ribos, ją galima spręsti sekančios atakos paieškos iteracijos metu.

4.3.2.7. Atakos prevencija

Palyginus atakas su nustatytomis ribinėmis vertėmis galime pradėti ieškotis būdų kaip užkirsti joms kelią.

Dažnu atveju atakoms įgyvendinti yra išnaudojami netobulumai sistemos naudojamuose procesuose ar iš anksto neatrastos klaidos. Pvz. galima pavišinti rinkimų aplikaciją tik pirmą rinkimų dieną, o ne iš anksto. Tačiau šis sprendimas dažniausiai būna įtakotas politinio sprendimo, dėl to sunku jį greitai pakeisti.

5. Modelio pritaikymas

Šiame skyriuje pasiūlytas modelis bus pritaikytas Estijos elektronei balsavimo sistemai. Estija pasirinkta dėl to, jog yra pavišinusi daug statistikos apie elektronių balsavimą savo šalyje.

Bus trumpai aptartos bei išnagrinėtos dvi atakos:

- Vietos pirkimo Seime ataka. Ši ataka turėtų likti nepastebėta rinkimų organizatorių, kad būtų laikoma sėkmingai įgyvendinta;

- Ataka, kuri pažeidžia pasitikėjimą elektroninio balsavimo sistema. Bus siekiama pavišinti rinkėjų informaciją bei už ką jie balsavo, taip menkinant pasitikėjimą sistema..

5.1. Paieška

Bus aptarta dalis Estijos elektroninio balsavimo schemos, tačiau pats modelis nebus tikrinamas taikant NuSMV. Bus aptarta modelio dalis, kurią tiesiogiai naudoja galutinis vartotojas, t. y. balsavimo aplikacijos naudojimas/parsisiuntimas bei balso verifikacija.

5.1.1. Esysbės ir atributai

Ieškant esybų ar jų atributų labai patogu naudotis grafine schema (nuoroda į Estijos balsavimo schema 3 skyriuje). Galima lengvai išskirti tokias esybės, kaip balsavimo aplikacija, balsas, viešasis rinkimų organizatorių raktas, privatus pasirašymo raktas ir eID. Įsigilinus į eID veikimą, tampa akivaizdu, jog jai reikia PIN1 ir PIN2, kad ji galėtų veikti.

Nustačius esybės reikia nustatyti jų atributus. Patartina, jog juos padėtų nustatyti atitinkamos srities specialistai, bet dažniausiai esybės šiame kontekste turės bent lokacijos bei turinio atributus. Pradinėje darbų sekos (angl. *workflow*) stadijoje būtina nustatyti pradines atributų reikšmes (pvz. balsadėžės turinio atributo reikšmė būtų „tuščia“).

Esysbės, kurių atributai nėra valdomi procesų, Estijos balsavimo schemeje yra išorinis rinkimų organizatorių raktas, privatus pasirašymo raktas, PIN1, PIN2, sesijos ID, atsitiktinis dydis ir kompiuterinis įrenginys. Nors šių esybų tiesiogiai neįtakoja procesai, tačiau jos gali būti suklastos arba turėti netikrus duomenis.

Esysbės, kurių atributai yra įtakojami procesų, yra balsas, balsavimo aplikacija ir eID.

5.1.2. Procesai

Išanalizavę keletą procesų galime nustatyti keletą procesų, kaip *įvesti balsą į balsavimo aplikaciją, užšifruoti balsą, perduoti balsą į eID, pasirašyti balsą bei siųsti balsą į balsų apdorojimo serverį.*

Estijos balsavimo sistema palaiko balsų verifikavimą, naudojant QR kodus. Norint, jog tai veiktų, serveriui reikia *sugeneruoti sesijos ID*, balsavimo aplikacijai reikia *sugeneruoti atsitiktinį skaičių*, *sugeneruoti QR kodą* ir *atvaizduoti QR kodą galutiniame įrenginyje*.

5.2. Skaidymas

Prieš tai nustatytos atakos (vietos Seime pirkimo bei pasitikėjimo sistema) šiame poskyryje bus išskaidytos. Bus sudarytas detalus atakos medis, apskaičiuota, kiek reikės resursų bei kokia galima atakos kaina.

5.2.1. Vietos Seime pirkimo ataka

Šios atakos įgyvendinimas susideda iš sekančių žingsnių: *pakeisti balsą į suklastotą balsą*, *pakeisti sesijos ID ir atsitiktinį skaičių*, kad suklastoti verifikaciją.

5.2.1.1. Atakos medis

Norint pakeisti du minėtus procesus veiksmų sekoje (angl. *workflow*), būtina nustatyti, kur jie vyksta. Abu procesai vykdomi rinkėjo naudojamoje balsavimo aplikacijoje, kuri veikia rinkėjo kompiuteryje. Vienas iš būdų būtų įterpti į balsavimo aplikaciją kenkėjišką kodą. Kenkėjo tikslas bus vienos vietos Seime „nupirkimas“.

Atakos medį sudaranti struktūra ir sąnaudos:

C&C (angl. *Command-and-Control*) infrastruktūra

- Apsaugoti C&C serveriai – vienas serveris aptarnauja daugiausia 3500 aktyvių rinkėjų;
- Apsaugotas C&C valdymo serveris;
- Anoniminis VPN (angl. *Virtual Private Network*), skirtas prisijungimui prie valdymo serverio;
- Supaprastintas zombių tinklo (angl. *botnet*) valdymo kodas;
- Zombių tinklo konsultacija.

Talpyklos kenkėjiškas kodas

- Kenkėjiškas kodas, kuris saugos vietą iki kol bus atsiųsta pakeista balsavimo aplikacija;
- Talpyklos kodo pakeitimai.

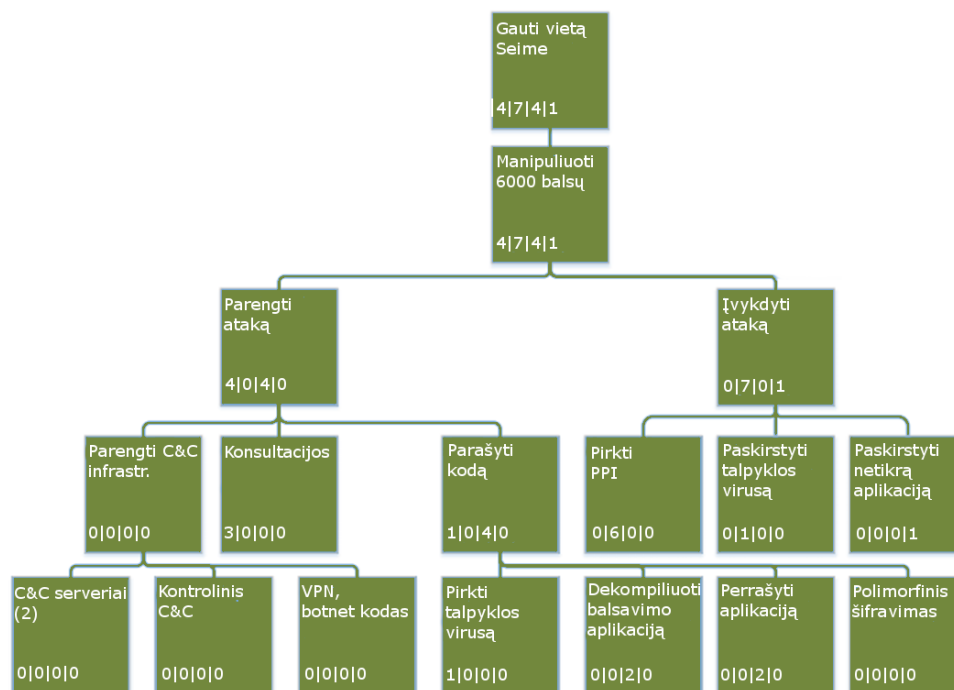
Pati kenkėjiška programa bus sukurta dekompilijuojant balsavimo aplikaciją bei ją perrašant. Kenkėjiška aplikacija bus užšifruota polimorfiniu šifruotoju, kad antivirusinės programos jos neaptiktų:

- Dekompilijuoti balsavimo aplikaciją;
- Sukurti kenkėjišką aplikaciją;
- Sukonfigūruoti zombių tinklą aplikacijos skirstymui;
- Polimorfiškai užšifruoti aplikaciją, kad vieną aplikacijos „versiją“ turėtų ne daugiau nei 1000 kompiuterių.

Kad sumažinti įtarimą, kai bandoma verifikuoti labai daug vieno rinkėjo balsų, būtų galima keisti tik dalį balsų, tačiau rinkti informaciją apie rinkėjus, jų naudotus sesijos ID bei sugeneruotus atsitiktinius skaičius, kuriuos vėliau galima perpanaudoti.

5.2.1.2. Dienos

Skirtingi atakos medžiai žingsniai gali būti papildyti dienų, reikalingų jiems įgyvendinti skaičiumi, kurios buvo aptartos prieš tai. Papildytas atakos medis pavaizduotas 8 pav.



8 pav. Papildytas vietos pirkimo Seime atakos medis (dienomis)

Laiko sąnaudos yra suskirstytos į aktyvias ir pasyvias prieš ir po balsavimo periodo dienas. Medyje dienos pateiktos šiuo formatu: Aktyvios prieš rinkimų periodą | Pasyvios prieš rinkimų periodą | Aktyvios per rinkimų periodą | Pasyvios per rinkimų periodą.

5.2.1.3. PPI

Kad sėkmingai „nupirkti“ bent vieną vietą Estijos Seime, kenkėjai reikia pakeisti apie 6000 balsų (101 vieta Seime – balsą atiduoda apie 600000 rinkėjų) [42]. Kad nustatyti kiek PPI (angl. *Pay-per-install*) reikia pirkti, kad 6000 kompiuterių būtų panaudoti rinkimuose, reikia nustatyti kiek kompiuterių buvo vidutiniškai naudojama elektroniniam balsavimui.

Kompiuterių skaičius Estijoje

Estijos įmonėse, 47,5 % darbuotojų naudoja kompiuterius, tai reiškia, jog 621 300 žmonių tenka 295 118 darbo kompiuterių [43]. Tačiau nepavyko rasti duomenų apie Estijoje turimų kompiuterių skaičių namuose, tačiau rasta informacija apie Suomiją – 1.6 kompiuteriai per namų ūkį [42]. Iš to seka,

kad 600 000 Estijos namų ūkių turi apie 960 000 kompiuterius. Tai susiveda į 1,255 milijono kompiuterių Estijoje.

Vidutinis rinkėjų skaičius, naudojančių elektroninį balsavimo būdą

Iš visų balso teisę turinčių rinkėjų, apie 15 % naudojo elektroninį balsavimą – 163 035 rinkėjai [42], iš kurių, spekuliuojant, 80 % naudojo namų kompiuterius, 20 % darbinius:

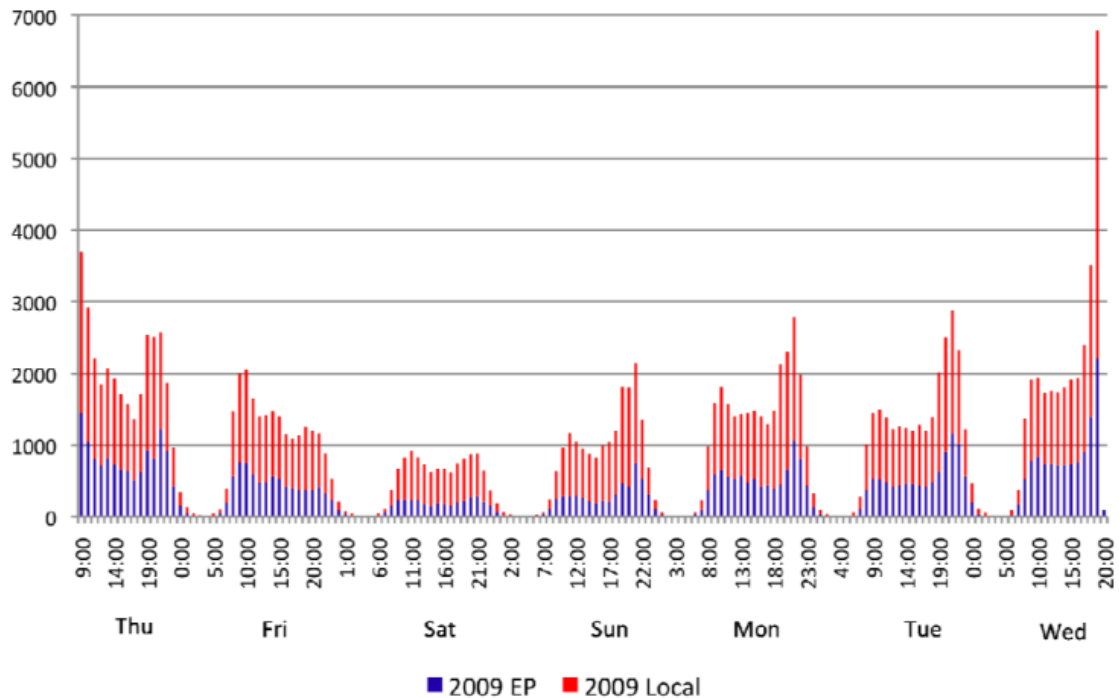
- Namuose balsavę rinkėjai sudaro $163\,035 * 0.8 = 130\,428$ iš galimų 960 000 kompiuterių;
- Darbe balsavę rinkėjai sudaro $163\,035 * 0.2 = 32\,607$ iš galimų 490 000 kompiuterių.

Iš to galime išvesti formulę ir paskaičiuoti naudotų kompiuterių elektroniniame balsavime procentą:

$$\frac{\text{Namuose balsavę rinkėjai}}{\text{Namų kompiuteriai}} * \frac{\text{Namų kompiuteriai}}{\text{Visi kompiuteriai}} * 100 \% + \frac{\text{Darbe balsavę rinkėjai}}{\text{Darbe esantys kompiuteriai}} * \frac{\text{Darbe esantys kompiuteriai}}{\text{Visi kompiuteriai}} * 100 \% = \frac{130\,428}{960\,000} * \frac{960\,000}{1\,255\,000} * 100 \% + \frac{32\,607}{490\,000} * \frac{490\,000}{1\,255\,000} * 100 \% = 12,99 \%$$

Tai reiškia, jog norint pakeisti 6000 balsus, reikia užkrėsti bent 46 189 Estijos kompiuterius (pirkti PPI). Kadangi elektroniniam balsavimui naudojamų kompiuterių pasiskirstymas nėra tolygus (kai kuriuose namų ūkiuose jie gali būti aktyviau naudojami, nei kituose), šio darbo kontekste imsime 20 %, o ne 15 % elektroniniu būdu balsavusių rinkėjų. Tai reiškia, jog bendras perkamų užkrėstų kompiuterių skaičius padidėja iki 56 000.

Kadangi Estijoje elektroninio balsavimo periodas yra 7 dienos, o pasiruošti atakai (dekompiliuoti aplikaciją, ją pakeisti bei paskirstyti kenkėjišką aplikaciją) trunka 5 dienas, reikia nustatyti, koks skaičius rinkėjų balsuos per paskutines dvi dienas. 9 pav. pateiktas rinkėjų aktyvumas naudojant elektroninį balsavimą valandomis.



9 pav. Estijos elektroninio balsavimo balsų pasiskirstymas pagal valandas [39]

Pagal 2011 metų statistiką, iš 140 000 balsų atidavusių e. rinkėjų 51 000 balsavo paskutines dvi dienas [39] – tai 36,43 %.

Tai reiškia, kad kenkėjui iš viso reikia $\frac{56\,000}{0.3643} * 100 \% = 153\,719$ užkrėstų kompiuterių.

Svarbu įvertinti ir tai, jog yra ribotas kiekis šalyje užkrėstų kompiuterių, dėl to šios atakos kontekste galima susidurti su tam tikromis ribomis. Apsidraudimo vardan bus laikoma, jog reikia 170 000 užkrėstų kompiuterių.

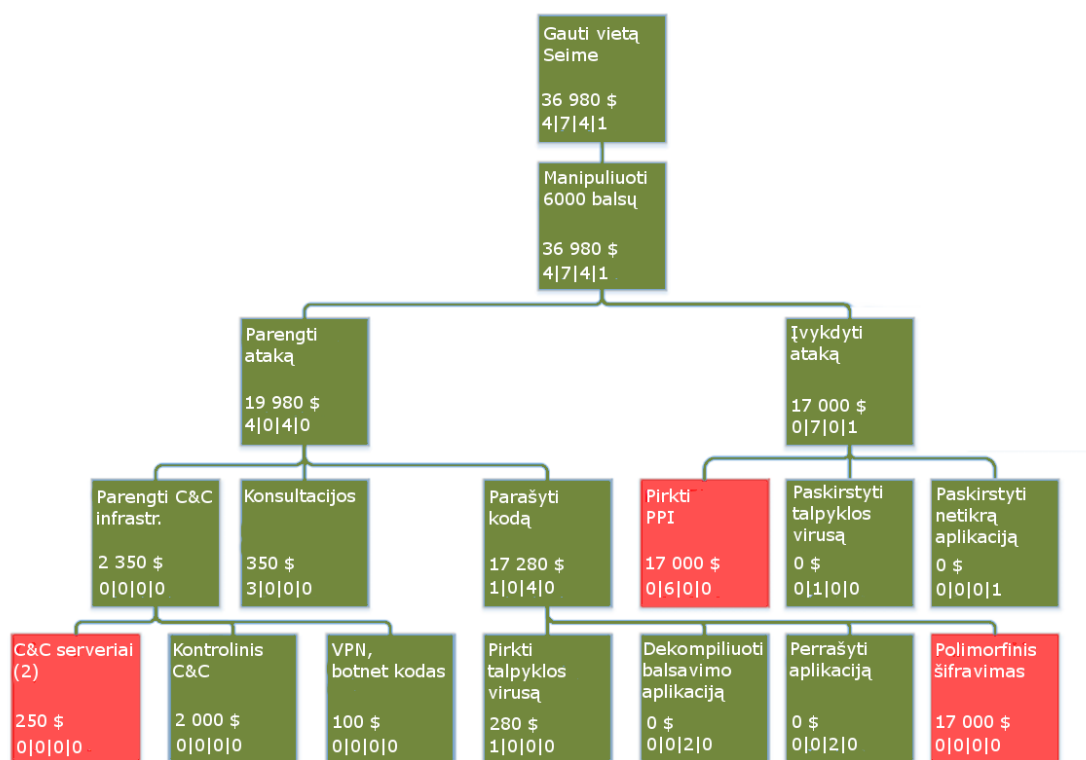
5.2.1.4. Kaina

Bus laikoma, jog visi atakai skirti komponentai bus pirkti šešėlinėje rinkoje ir kad kenkėjišką programinę įrangą kuriantis asmuo yra patyręs programuotojas, tačiau prieš tai nebuvo vykdęs panašaus masto atakos ir jam reikia konsultacijos, kaip sukonfigūruoti zombių tinklą (angl. *botnet*). Paslaugų ir komponentų kaina pateikta 4 lentelėje.

4 Lentelė. Komponentų vietos Seime pirkimo atakai įgyventi kainos [38]

Komponentas	Kintančios / Fiksuotos	Kaina (USD)
C&C serveriai (2)	Kintančios	250
C&C valdymo serveris	Fiksuotos	2000
Anoniminis VPN	Fiksuotos	30
Supaprastintas zombių tinklo kodas	Fiksuotos	70
Zombių tinklo konsultacijos	Fiksuotos	350
Talpyklos kenkėjiškas kodas	Fiksuotos	250
Zombių tinklo ir kenkėjiškos programinės įrangos apjungimas	Fiksuotos	30
Polimorfinis šifruotojas (170 kartų)	Kintančios	17000
170 000 PPI	Kintančios	17000

Turint komponentų kainas bei laiko sąnaudas, galime papildyti atakos medį, kuriame pateiktos ir kainos.



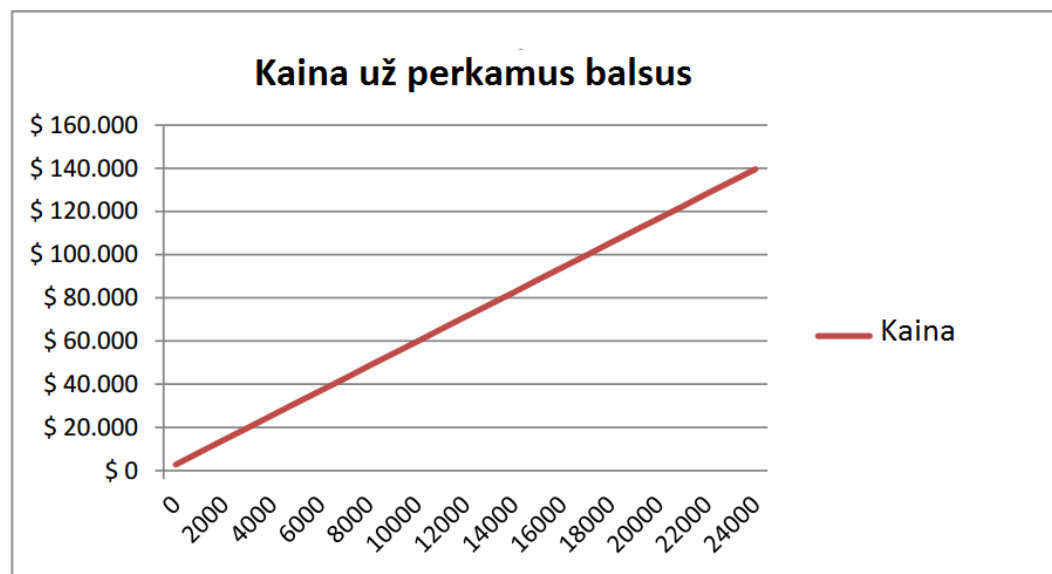
10 pav. Pilnas atakos medis vietos Seime pirkimo atakai

Turint šią informaciją galima gana paprastai parašyti kainos atakai funkciją. Raudoni atakos medžio mazgai žymi kintančias išlaidas, žali – fiksuotas. Kaip minėta anksčiau, 6000 balsų reikia nupirkti apie 170 000 PPI ir kas 3500-am kompiuteriui reikia vieno C&C serverio.

$$Kaina = Kontrolės\ serveris + VPN\ ir\ botnet + Botnet\ Konsultacija + 125 * \frac{Balsai}{3500} + Talpyklos\ kodas + \frac{17000}{6000} * Balsai + \frac{17000}{6000} * Balsai$$

$$Kaina = 2000 + 100 + 350 + 125 * \frac{Balsai}{3500} + 280 + \frac{17000}{6000} * Balsai + \frac{17000}{6000} * Balsai$$

$$= 2730 + 125 * \frac{Balsai}{3500} + 5\frac{2}{3} * Balsai$$



11 pav. Vietos pirkimo Seime atakos kaina pagal klastotų balsų skaičių.

Iš pateikto grafiko matome, jog užtenka apie 37 000 \$, kad nupirkti vieną vietą Seime.

5.2.1.5. Vietos Seime pirkimo išvados

Kaip matome, finansinės išlaidos nupirkti vieną vietą Seime išnaudojant elektroninio balsavimo Estijoje trūkumus yra gana mažos. Pasiruošti atakai kainuoja apie 2730 \$, o įtraukiant kintančias išlaidas (6000 balsų pirkimui), gauname, jog reikia apie 37000 \$.

Laiko sąnaudos taip pat nėra didelės, kadangi pasiruošimo laikas motyvuotam kenkėjui gali būti begalinis. Iš esmės svarbus tik laikas, kuris sugaištas per rinkimų periodą, kuris šios atakos atveju siekia 5 dienas.

Šią ataką galime laikyti galima, tačiau esant ribai, kiek užkrėstų kompiuterių galima nusipirkti, atsiranda riba, kiek vietų Seime galima nupirkti.

5.2.2. Ataka prieš pasitikėjimą sistema

Dar viena iš galimų atakų yra nukreipta į pasitikėjimo sistema mažinimą. Galima atrasti nemažai būdų, kaip tai gyvendinti, tačiau poskyryje bus aptarta situacija, kai kenkėjas pavogia rinkėjo duomenis bei už ką jį balsavo ir paviešina duomenis internete.

Kad ši ataka būtų laikoma sėkminga, bus siekiama atkreipti visuomenės dėmesį viešinant duomenis, taip keliant nepasitikėjimą rinkimų sistema. Bus laikoma, jog kenkėjas paviešins naujai pavogtą balsą kas atitinkamą laiko tarpą

5.2.2.1. Atakos medis

Atakos medis šiai atakai yra beveik toks pat, kaip ir vietos Seime pirkimo atveju. Kenkėjui reikės dekompiliuoti ir pakeisti balsavimo aplikaciją. C&C infrastruktūra bus ta pati, tik vietoje sesijos ID ir atsitiktinių skaičių valdymo ji atliks rinkėjo informacijos saugojimo ir apdorojimo ir darbus. Vienintelis papildomas žingsnis yra balsų viešinimas.

5.2.2.2. Dienos

Kadangi atakos medis nedaug kuo skiriasi nuo prieš tai aptartos atakos, nėra didelių pokyčių ir laiko sąnaudose. Esminis skirtumas yra, jog sukurti balsų keitimo procedūras yra sunkiau nei sukurti balsų

vogimo procedūras. Bus laikoma, jog pritaikyti balsavimo aplikaciją balsų vogimui užteks tik 1 dienos vietoje 2.

5.2.2.3. PPI

Priklausomai nuo to, kiek balsų kenkėjas nori paviešinti, atitinkamai kinta ir reikalingų užkrėstų kompiuterių skaičius.

Nors Estijos elektroninio balsavimo periodas yra gana trumpas (7 dienos), iš 9 pav. (laiko grafikas kada balsuota) matome, jog balsų pasiskirstymas per dieną nėra visiškai tolygus. Kad būtų įmanoma paviešinti po balsą kas valandą, kenkėjui, apsidraudžiant, reiktų turėti maždaug 24 balsų rezervą, jei kartais nei vienas iš jo užkrėstų kompiuterių nebus naudojami elektroniniam balsavimui. Be kita ko kenkėjas gali pradėti rinkti balsus tik tada, kai paviešina kenkėjišką balsavimo aplikaciją.

Kadangi kenkėjas 3 dienas ruoš kenkėjišką aplikaciją, jis galės pradėti rinkti balsus tik ketvirtą rinkimų dieną. Vidutiniškai ketvirtą rinkimų dieną balsuoja apie 18000 rinkėjų iš 142 000 [42] tai dariusių per visą periodą. Iš to seka, kad kenkėjui reikia

$$\frac{24}{\frac{18000}{142000}} \approx 190$$

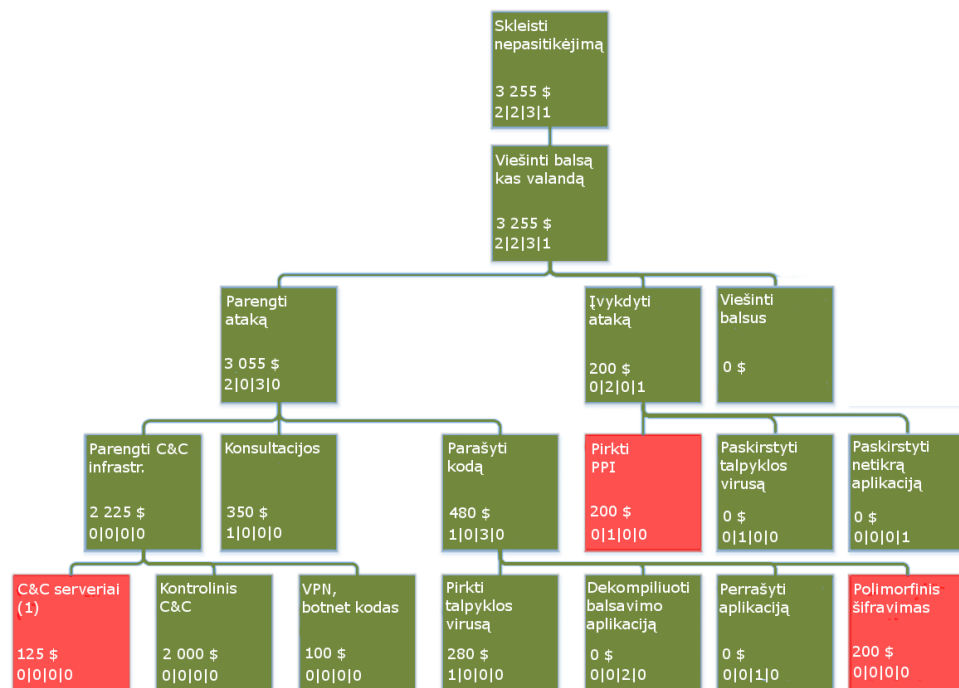
rinkėjų per dieną. Kad užtikrinti, jog tikrai pavyks užkrėsti tiek rinkėjų kompiuterių, galima pasinaudoti prieš tai aptartos atakos skaičiavimais. 36,43% rinkėjų reikėjo $\frac{170000}{6000}$ užkrėstų kompiuterių, tad norint jog ši ataka būtų sėkminga reikia

$$190 * \frac{170000}{6000} * \frac{36,43\%}{100\%} \approx 1,961$$

užkrėstų kompiuterių.

5.2.2.4. Kaina

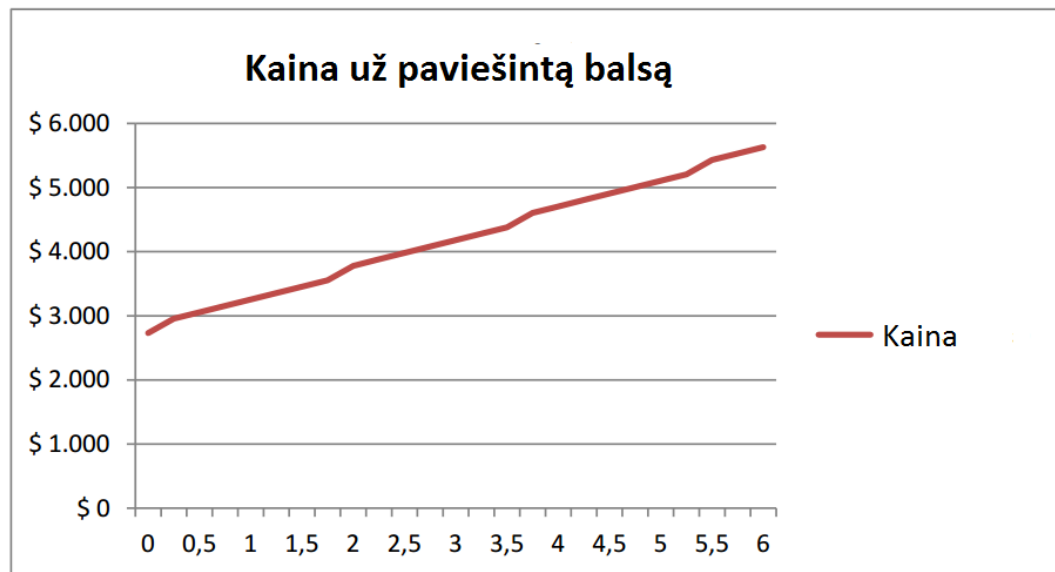
Komponentų atakai įgyvendinti kainos tokios pat kaip ir vietos Seimo pirkimo atakos, nepaisant kintančių išlaidų, t. y. PPI pirkimo, polimorfinio šifravimo ir C&C serverių. Pilnas atakos medis pavaizduotas 12 pav.



12 pav. Atakos prieš pasitikėjimą rinkimų sistema atakos medis

Kaip nagrinėta anksčiau, reikalingų aukų skaičius nėra lygus reikiamam užkrėstų kompiuterių pirkimui. Apvalinant laikysime, jog reikia 2000 užkrėstų kompiuterių, kas 3500-tam kompiuteriui reikia vieno C&C serverio. Kas 1000-ajam kompiuteriui reikia atlikti naują polimorfinį šifravimą. Visos kitos išlaidos yra fiksuotos. Iš to galime parašyti nesudėtingą kainos funkciją

$$\begin{aligned}
 \text{Kaina} &= \text{Kontrolės serveris} + \text{VPN ir botnet} + \text{Botnet Konsultacija} + 125 * \frac{\text{Balsai} * 2000}{3500} \\
 &+ \text{Talpyklos kodas} + 200 * \text{Balsai} + 200 * \text{Balsai} \\
 \text{Kaina} &= 2730 + 125 * \frac{\text{Balsai} * 2000}{3500} + 400 * \text{Balsai}
 \end{aligned}$$



13 pav. Pasitikėjimo prieš rinkimų sistemą atakos kaina, norint paviešinti atitinkamą balsų skaičių per valandą

5.2.2.5. Atakos prieš pasitikėjimą sistema išvados

Kaip matome, finansinės sąnaudos šiai atakai įgyvendinti yra labai mažos. Užtenka apie 2730 \$, kad pasiruošti atakai, bei apie 600\$ už kiekvieną paviešinamą balsą per valandą. Pakanka apie 3255 \$, kad paviešinti po vieną balsą kas valandą, kas jau gali sukelti rimtas pasekmes įtakojančias pasitikėjimą sistema. Laiko sąnaudos taip pat nėra didelės – motyvuotam kenkėjui laikas prieš rinkimų periodą yra neribotas (pasiruošimui), o per rinkimų periodą pakanka trijų dienų.

5.3. Palyginimas

Sudarius skirtingų atakų medžius bei pasirašius jų sąnaudų (kainos) funkcijas, galime jas palyginti bei atsakyti į klausimą, kuri ataka labiau tikėtina? Laikoma, jog kuo ji pigesnė – tuo ji labiau tikėtina.

$$\text{Vietos seime pirkimo atakos kaina} = 2730 + 125 * \frac{\text{Balsai}}{3500} + 5\frac{2}{3} * \text{Balsai}$$

$$\text{Atakos prieš pasitikėjimą kaina} = 2730 + 125 * \frac{\text{Balsai} * 2000}{3500} + 400 * \text{Balsai}$$

Kadangi vietos Seime pirkimo atakos atveju reikia daug daugiau balsų, ji yra brangesnė įgyvendinti, tačiau tikėtina, labiau įtakojanti patį rinkimų procesą.

5.4. Prevencija

Aptikus ir įvertinus atakas galima pradėti spręsti jų prevencijos klausimus. Pvz. vietos Seime pirkimo atakos atveju būtų galima patobulinti balsų verifikacijos mechanizmą. Vienas iš variantų, jei balsuojama ir autentikuojamasi naudojant mobilųjį įrenginį, būtų papildoma verifikacija siunčiant SMS žinutę, numerį gaunant iš telefone esančios SIM kortelės. Tačiau šis papildomas verifikacijos žingsnis kainuotų gana nemažai, ypač jei rinkėjai aktyviai perbalsuoja.

6. Rezultatai ir išvados

Atlikus darbą galima išskirti sekančius rezultatus:

1. Išanalizuoti bei suformuluoti reikalavimai elektroninio balsavimo sistemai;
2. Pasirinktos ir išanalizuotos 3 šiuo metu veikiančios elektroninio balsavimo sistemos – Estijos, Prancūzijos ir Norvegijos;
3. Išanalizuotos potencialaus kenkėjo galimybės prieš elektroninio balsavimo sistemą. Analizė atlikta remiantis Weldermariam ir Villarforita pasiūlytu būdu, kuriant atakos medžius;
4. Pasiūlytas elektroninės balsavimo sistemos tikrinimo modelis, susidedantis iš elektroniniame balsavime naudojamų esybių analizės, atakos medžių kūrimo, statistikos surinkimo bei kainos įvertinimo;
5. Pasiūlytas saugumo tikrinimo modelis pritaikytas Estijos elektroninio balsavimo sistemai. Didžioji analizės dalis buvo nukreipta į modelio skaidymo žingsnį, kuriame detalai nagrinėjama atakos sandara bei sąnaudos. Atlikti skaičiavimai remiasi tuo, jog yra įmanoma įsigyti gana daug užkrėstų kompiuterių (vietos Estijos Seime pirkimo atveju – 170000). Būtent šis parametras riboja galimą atakos dydį.

Atlikus darbą galima išskirti sekančias išvadas:

1. Išnagrinėjus keletą šiuo metu veikiančių elektroninio balsavimo sistemų pastebėta, jog tik Estija leidžia dalyvauti visuose galimuose rinkimuose elektroniniu būdu bei turi pateikusi daugiausia statistikos bei informacijos apie savo sistemą;
2. Išnagrinėjus galimus balsų pirkimo/pardavimo prevencijos sprendimus galima teigti, jog elektroninio balsavimo taikymas leidžia kovoti su balsų pirkimu bei apsaugoti rinkėjus nuo jų duomenų vagystės;
3. Atlikus kenkėjo atakos galimybių analizę nustatyta, jog yra realu įvykdyti ataką bandant užkrėsti galinių vartotojų kompiuterius. Atakos infrastruktūros kaina nėra didelė (apie 3000 \$);
4. Taikant siūlomą modelį elektroninio balsavimo schemai remiantis Weldermariam ir Villafiorita technika pastebėta, jog galima pakankamai nesudėtingai apsirašyti esybių ir ryšių diagramą, kurią vėliau galima naudoti detalesnei analizei;
5. Atlikus tyrimą, pastebėta, jog atakos medžių naudojimas leidžia paprastai ir suprantamai pateikti atakos struktūrą bei poreikius;

6. Turint prieigą prie elektroninio balsavimo statistikos bei informacijos apie kenkėjo galimai patiriamas išlaidas galima nesudėtingai paskaičiuoti galimų atakų kainą. Tikėtina, jog dauguma atakų naudos panašią infrastruktūrą, dėl to galima greitai pritaikyti seną atakos medį naujai atakai;

7. Detaliau išnagrinėjus keletą atakų nustatyta, kad surengti ataką prieš kartinę demokratijos procesą nėra brangu. Pavyzdžiui, kad nupirkti vieną vietą Estijos Seime pakanka apie 37 000\$, o atakai prieš pasitikėjimą sistema pakaktų apie 3300 \$.

Literatūros sąrašas

1. Hof S. *E-Voting and Biometric Systems*. [žiūrėta 2016-05-16]. Prieiga per internetą: https://www.researchgate.net/profile/Robert_Krimmer/publication/220789172_Security_Assets_in_E-Voting/links/0912f50cb2746f2e89000000.pdf >
2. Lepp U.; Loide E. 2007. *E-Voting – A Key to Independence for All*. [žiūrėta 2016-01-09]. Prieiga per internetą: <http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-415/paper10.pdf>
3. E-Democracy. *Goals and Objectives DRAFT 0.9*. [žiūrėta 2016-01-09]. Prieiga per internetą: <http://www.e-democracy.org/objectives.html>
4. Schneier B. 2000. *Voting and Technology*. [žiūrėta 2016-01-09]. Prieiga per internetą: <http://www.notablesoftware.com/Press/Schneier.html>
5. ISO/IEC 27002:2013. [žiūrėta 2016-05-22]. Prieiga per internetą: <http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf>
6. *Balsavimo internetu rinkimuose ir referendumuose koncepcija*. [žiūrėta 2016-05-18]. Prieiga per internetą: <http://www3.lrs.lt/docs2/HUJQOGCB.DOC>
7. *Legal, operational and technical standards for e-voting*. [žiūrėta 2016-05-18]. Prieiga per internetą: [http://www.coe.int/t/dgap/democracy/Activities/Key-Texts/Recommendations/Rec\(2004\)11_Eng_Evoting_and_Expl_Memo_en.pdf](http://www.coe.int/t/dgap/democracy/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf)
8. *Lietuvos Respublikos vyriausiosios rinkimų komisijos pirmininko ataskaita*. [žiūrėta 2016-05-18]. Prieiga per internetą: <http://www3.lrs.lt/docs2/REGOBIUT.DOC>
9. *Lietuvos Respublikos Prezidento rinkimų įstatymas*. [žiūrėta 2016-05-18]. Prieiga per internetą: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=267498
10. *Lietuvos Respublikos elektroninio parašo įstatymas*. [žiūrėta 2016-05-18]. Prieiga per internetą: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=105849
11. *Lietuvos Respublikos Seimo rinkimų įstatymas*. [žiūrėta 2016-05-18]. Prieiga per internetą: http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=267672
12. *Summary of the problem with Electronic Voting*. [žiūrėta 2016-05-19]. Prieiga per internetą: http://www.verifiedvoting.org/wp-content/uploads/downloads/revised_summary31.pdf
13. *e-häätamise tarkvara (angl. e-voting software)*. [žiūrėta 2016-05-21]. Prieiga per internetą: <https://github.com/vvk-ehk/evalimine>

14. Gerlach J.; Gasser U. *Three Case Studies from Switzerland: E-Voting*. [žiūrėta 2016-05-21]. Prieiga per internetą: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf
15. Volkamer M.; Vogt R. 2008. *German Research Center for Artificial Intelligence. Core Requirements for Online Voting Systems. Protection profile*. [žiūrėta 2016-05-21]. Prieiga per internetą: https://books.google.lt/books?id=6Y1mCaqv_TUC&pg=PA151&lpg=PA151&dq=Volkamer+Core+Requirements+for+Online+Voting+Systems&source=bl&ots=1ZsT8yoHXG&sig=tvk33F5GwNyI0QMJaALDGIreitM&hl=en&sa=X&ved=0ahUKEwjnrHF5-3MAhXiB5oKHa54CxcQ6AEILjAB#v=onepage&q=Volkamer%20Core%20Requirements%20for%20Online%20Voting%20Systems&f=false
16. Grimm R.; Volkamer M. *Development of a Formal IT Security Model for Remote Electronic Voting Systems*. [žiūrėta 2016-05-21]. Prieiga per internetą: <https://www.semanticscholar.org/paper/Development-of-a-Formal-IT-Security-Model-for-Volkamer-Grimm/5fe94f2ca49782b8469844c3e0b1e0dadde279e4/pdf>
17. Miškinis R. *Elektroninė laiko žymė*. [žiūrėta 2016-05-21]. Prieiga per internetą: http://rtn.elektronika.lt/rtn/0102/laiko_zyme.html
18. *Constitutionality of Remote Internet Voting: The Estonian Perspective*. [žiūrėta 2016-05-22]. Prieiga per internetą: <http://www.juridicainternational.eu/?id=14845>
19. Rivest R. *Electronic Voting*. [žiūrėta 2016-05-22]. Prieiga per internetą: <http://people.csail.mit.edu/rivest/Rivest-ElectronicVoting.pdf>
20. Lundin D. *Simple and Secure Electronic Voting with Prêt à Voter*. [žiūrėta 2016-12-10]. Prieiga per internetą: <https://www.semanticscholar.org/paper/Simple-and-Secure-Electronic-Voting-with-Pr-t-Lundin/1db4237644727c5d1d4b9f453e1eabe3b6cab799/pdf>
21. Chau H. *Network Security – Defense Against DoS/DDoS Attacks*. [žiūrėta 2016-12-10]. Prieiga per internetą: http://www.leetupload.com/database/Misc/Papers/Asta%20la%20Vista/defense_ddos.pdf
22. Žodynas.lt. [žiūrėta 2016-12-11]. Prieiga per internetą <http://www.zodynas.lt/terminu-zodynas/S/sertifikavimas>
23. Barrat i Esteve. *The Certification of E-Voting Mechanisms. Fighting against Opacity*. [žiūrėta 2016-12-11]. Prieiga per internetą: http://www.evoting.cc/wpcontent/uploads/Proceedings%202008/6.2.Barrat_presentation.pdf, Dokumentas: <http://www.ordinateurs-de-vote.org/IMG/jpg/cada.jpg>

24. *Security criteria for electronic voting*. [žiūrēta 2016-12-18]. Prieiga per internetą: <http://www.csl.sri.com/users/neumann/ncs93.html>
25. *Estonia Parliamentary Elections 1 March 2015 OSCE/ODIHR Needs Assessment Mission Report*. [žiūrēta 2016-05-22]. Prieiga per internetą: <http://www.osce.org/odihr/elections/estonia/139566?download=true>
26. VKA. *Onderzoek internetstemmen voor kiezers in het buitenland. Technical report*. [žiūrēta 2017-03-12]. Prieiga per internetą: <https://zoek.officielebekendmakingen.nl/blg-286503.pdf> >
27. Madise U.; Martens T. 2005. *E-voting in Estonia. The first practice of country-wide binding internet voting in the world. Electronic voting*. [žiūrēta 2017-03-12]. Prieiga per internetą: https://www.researchgate.net/publication/220764757_E-voting_in_Estonia_2005_The_first_Practice_of_Country-wide_binding_Internet_Voting_in_the_World
28. Dreier J.; Lafourcade P.; Lakhnech Y. *A formal taxonomy of privacy in voting protocols. In Communications (ICC)*. [žiūrēta 2017-03-19]. Prieiga per internetą: <http://sancy.univ-bpclermont.fr/~lafourcade/SLIDES/ICC-SFCS12.pdf>
29. Juels A.; Catalano D. *Coercion resistant electronic elections. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. [žiūrēta 2017-03-19]. Prieiga per internetą: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.8089&rep=rep1&type=pdf>
30. Grewal G.; Ryan D.; Bursuc S.; Caveat R.. 2013. *Coercion-evidence in electronic voting. In IEEE Security and Privacy Symposium*. [žiūrēta 2017-03-19]. Prieiga per internetą: <http://gurchetan.com/papers/caveatcoercitor.pdf>
31. Moran T.; Naor M.. 2006 *Receipt-free universally-verifiable voting with everlasting privacy. In Advances in Cryptology CRYPTO 2006*, 373–392p. [žiūrēta 2017-03-19]. Prieiga per internetą: <http://www.iacr.org/cryptodb/archive/2006/CRYPTO/1914/1914.pdf>
32. Martens T.. 2010. *Internet voting in Estonia. Technical report*. [žiūrēta 2017-03-20]. Prieiga per internetą: http://lata.org.lv/wp-content/conf/Drosiba/LATA_EST_iVelesanas_TarviMartens.pdf
33. Heiberg S.; Laud P.; Willemson J. 2011. *The application of i-voting for estonian parliamentary elections of 2011. In EVoting and Identity*. [žiūrēta 2017-03-20]. Prieiga per internetą: <https://research.cyber.ee/~janwil/publ/evote2011.pdf>

34. JB i Esteve; Goldsmith B.; Turner J. 2012. *International Experience with E-Voting - Norwegian E-Vote Project*. [žiūrēta 2017-03-21]. Prieiga per internetą: <<https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf>>
35. Pinault T.; Courtade P. 2012. *E-voting at expatriates mps elections in france*. In *Electronic Voting*. [žiūrēta 2017-03-21]. Prieiga per internetą: <<http://cs.emis.de/LNI/Proceedings/Proceedings205/189.pdf>>
36. Spycher O.; Volkamer M.; Koenig R. *Transparency and technical measures to establish trust in norwegian internet voting*. In *E-Voting and Identity*. [žiūrēta 2017-03-22]. Prieiga per internetą: <<https://pdfs.semanticscholar.org/520f/84270d78a8946ab7a1f24080b6ecd209f423.pdf>>
37. Storer T.; Duncan I. Polsterless. *Remote electronic voting*. *Journal of E-Government*. [žiūrēta 2017-03-23]. Prieiga per internetą: <<http://www.dcs.gla.ac.uk/~twspapers/storer04polsterless.pdf>>
38. Balzarotti, D. *An Experience in Testing the Security of Real-World Electronic Voting Systems*. [žiūrēta 2017-03-23]. Prieiga per internetą: <<http://ieeexplore.ieee.org/document/5210119/>>
39. Trechsel A.; Vassil K. 2010. *Internet voting in Estonia-A comparative analysis of four elections since 2005*. [žiūrēta 2017-03-31]. Prieiga per internetą: <[http://cadmus.eui.eu/bitstream/handle/1814/15688/Report - E-voting in Estonia 2005-2009.pdf?sequence=2&isAllowed=y](http://cadmus.eui.eu/bitstream/handle/1814/15688/Report_-_E-voting_in_Estonia_2005-2009.pdf?sequence=2&isAllowed=y)>
40. Dolev D.; Yao A. *On the security of public key protocols*. [žiūrēta 2017-04-01]. Prieiga per internetą: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.130.157&rep=rep1&type=pdf>>
41. Weldemariam K.; Villafiorita A. *Procedural security analysis: A methodological approach*. [žiūrēta 2017-04-02]. Prieiga per internetą: <https://www.usenix.org/legacy/event/evt08/tech/full_papers/weldemariam/weldemariam_html>
42. *Statistics about Estonian E-Voting*. [žiūrēta 2017-04-08]. Prieiga per internetą: <<http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>>
43. Data World Bank. [žiūrēta 2017-04-11]. Prieiga per internetą: <<http://data.worldbank.org/indicator/IT.NET.USER.P2?end=2017&locations=EE&start=2010>>

PRIEDAI

Priedas A. VGTU 20-osios jaunųjų mokslininkų konferencijos dalyvavimo pažymėjimas

