UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Ana Kosović

Bingo šema za elektronsko glasanje

Specijalistički rad

Podgorica, 2016. godina

UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Bingo šema za elektronsko glasanje

Specijalistički rad

Kriptografija

Mentor: Vladimir Božović

Ana Kosović

Matematika i računarske nauke

Podgorica, april 2016. godina

Apstrakt

Aktuelnost pitanja regularnosti izbornog procesa ne jenjava ni u 21. vijeku. U ovom radu je dat pregled osnovnih izazova koji utiču na pitanje povjerenja u izborni proces, kao i neki kriptografski odgovori na te izazove. U radu je poseban akcenat stavljen na *Bingo algoritam*. Ovaj sistem za elektronsko glasanje omogućava biraču neposrednu i tajnu provjeru da je njegov glas ubrojan odabranoj opciji. Ovim algoritmom se sprečavaju neke poznate manipulacije izbornog postupka kao što su podmetanje nepostojećih ili uništavanje pravih glasova. Takođe, predstavjeni su i mogući napadi na predstavljeni Bingo sistem za elektronsko glasanje.

Abstract

The question of regularity of the election process is still very actual even in the 21st century. This paper deals with the fundamental challenges which affect the question of confidence in the election process as well as with some cryptographic answers to these challenges. In this paper emphasis is put on the Bingo algorithm. This system of electronic voting allows voters to have a direct and confidential verification that his vote is properly attributed to the selected option. This algorithm can prevent some manipulations of the election process such as counting of non-existent votes or destruction of the real votes. The possible attacks on the Bingo electonic voting system will be also represented here.

Sadržaj

Glava 1

Uvod

Postepena pojava predsjedničkih vlasti u Evropi i Sjevernoj Americi, početkom 17. vijeka dovodi do pojave izbora u savremenom svijetu. U nekoj rudimentarnoj formi, izbori se pojavjuju i mnogo ranije, u Indiji, drevnoj Atini i Rimu.[1]

U srednjem vijeku pravo da glasaju na izborima imale su samo određene porodice, često na način da samo najstariji, muški član porodice glasa u ime svih ostalih članova porodice. Zakon o reformi iz 1832. godine, za posledicu je imao ukidanje glasačkih opština sa malim brojem stanovnika koje su kontrolisane od strane jedne osobe ili porodice. Zagovornici potpune demokratije zalagali su se za to da svi odrasli imaju pravo glasa.

Širom Zapadne Evrope i Sjeverne Amerike, pravo glasa punoljetnih muškaraca je bilo osigurano skoro svuda do 1920. godine, dok se glasačko pravo žena tek kasnije uspostavilo. Pravo da glasaju na izborima žene su dobije 1928. godine u Britaniji, 1944. godine u Francuskoj, 1946. godine u Crnoj Gori, 1949. godine u Belgiji i 1971. godine u Švajcarskoj.

Biračko tijelo može biti ograničeno formalno-pravnim zahtijevima. Primjer formalno-pravne barijere može biti da se neki glasač ne nalazi u biračkom spisku, iako zadovoljava sve uslove, pa ne može ostvariti pravo glasa. U mnogim zemljama na slobodnim izborima, veliki broj glasača ne glasa. Kao primjer možemo navesti Švajcarsku, gdje

više od pola glasačkog tijela obično ne koristi pravo glasa. Bez obzira na to što pojedini glasači ne mogu, a pojedini neće da ostvare pravo glasa, to ne umanjuje vrijednost odluke na izborima.

U ovom radu predstavićemo sve zastupljeniji vid glasanja – elektronsko glasanje, kao jednog od mehanizama da se animira što je moguće šira izborna populacija i spriječi korupcija izbornog sistema.

Glava 2

Preporuka Savjeta Evrope za elektronsko glasanje

Elektronsko glasanje (e-glasanje) predstavlja sintezu politike i tehnologije. Razvoj elektronskog glasanja moraju da prate odgovarajući standardi. Skup tih standarda obuhvata pravne i operativne standarde, kao i tehničke zahtjeve prilikom elektronskog glasanja. Primjena navedenih standarda predstavlja potvrdu da elektronsko glasanje može zamijeniti dosadašnji način glasanja.[2]

Komitet ministarstva Savjeta Evrope je 30. septembra 2004. godine usvojio dokument pod nazivom "*Preporuke Savjeta Evrope za pravne operativne i tehničke standarde pri sprovođenju elektronskog glasanja*". Dokument je donesen da bi zemlje članice Evropske unije imale načelno upustvo za sprovođenje elektronskih izbora. Navedeni dokument ne koriste samo članice Evropske unije koje organizuju elektronsko glasanje već i zemlje-kandidati kao što su: Moldavija, Ukrajina, Gruzija i druge. Ova preporuka je podijeljenja na tri dijela. Prvi dio se odnosi na pravne standarde i univerzalne principe slobode, jednakosti, kao i tajnosti u vezi sa pravom glasa. Drugi dio se odnosi na operativne standarde koji se primjenjuju na sve faze izbornog procesa, dok se treći dio odnosi na tehničke zahtijeve u vezi sa mogućnostima pristupa glasanju, bezbjednosti glasanja i kontrolom nad procesom glasanja.

Pravni standardi u preporuci Savjeta Evrope pod nazivom "*Pravni, operativni i*

tehnički standardi za elektronsko glasanje podijeljeni su na pravne principe i proceduralna pitanja.

2.1 Pravni principi

Univerzalno pravo glasa - glasački interfejs sistema e-glasanja mora biti razumljiv i lako uporedljiv; registacija glasača ne smije biti prepreka; e-glasanje mora biti osmišljeno tako da u što većoj mjeri omogućava glasanje osoba sa posebnim potrebama.

Jednako pravo glasa - u okviru izbora ili referenduma glasač će biti spriječen da glasa više od jednom koristeći elektronsku glasačku kutiju; svaki glas dat elektronskim putem računaće se samo jednom. Glasač će moći da glasa samo ako do tada nije glasao; svaki glas dat elektronskim putem računaće se samo jednom.

Sloboda glasanja - organizacijom e-glasanja obezbijediće se slobodno formiranje i izražavanje volje glasača; glasači će moći da promijene izbor tokom e-glasanja prije nego što konačno daju svoj glas; e-glasanje neće dozvoliti bilo kakav manipulativni uticaj na glasače tokom glasanja; e-sistem glasanja mora jasno pokazati da je glasač uspješno završio glasanje; e-sistem će spriječiti mijenjanje volje glasača nakon glasanja.

Tajnost glasanja - e-glasanje će biti tako organizovano da ni u jednoj fazi glasanja neće biti ugrožena tajnost glasanja; e-sistem glasanja će garantovati da će glasovi u elektronskim glasačkim kutijama ostati anonimni i da nije moguće rekonstruisati vezu između glasa i glasača; ?-sistem glasanja će biti tako dizajnirani da se rezultat glasanja u bilo kojoj elektronskoj kutiji ne može povezati sa pojedinačnim glasačem i da će biti preduzete sve mjere koje su potrebne kako bi se osiguralo da se informacije koje su potrebne tokom glasanja obrade.

2.2 Proceduralna pitanja

Proceduralna pitanja iz ove preporuke su:

Transparentnost - biće preduzete sve potrebne mjere da glasači razumiju e-sistem glasanja i da imaju povjerenje u taj sistem; informacije o funkcionisanju e-sistema glasanja moraju biti javno dostupne; glasači moraju da imaju mogućnost da vježbaju novi metod elektronskog glasanja prije nego što zaista glasaju; posmatračima će biti omogućeno da prisustvuju i nadgledaju elektronsko glasanje uključujući i dobijanje rezultata glasanja.

Verifikacija rezultata - sa komponentama elektronskog glasanja će biti upoznate nadležne izborne vlasti radi njihove provjere i sertifikacije, prije nego što elektronski sistem glasanja počne da radi; nezavisno tijelo, koje imenuje izborna vlast, treba da provjeri da li elektronski sistem glasanja radi ispravno i da li su preduzete sve mjere bezbjednosti; moraju biti verifikovane sve karakteristike e-sistema glasanja koje mogu da utiču na ispravnost rezultata glasanja; e-sistem glasanja ne smije sprečavati djelimično ili potpuno ponavljanje izbora ili referenduma.

Pouzdanost i bezbjednost - državni organi će obezbijediti pouzdanost i bezbjednost sistema e-glasanja; biće preduzeti svi koraci da se izbjegne mogućnost prevare ili da se neovlašćenom intervencijom utiče na sistem tokom cijelog procesa glasanja; e-sistem glasanja mora da sadrži mjere za stalno fukcionisanje sistema bez obzira na kvarove i napade sistema, prije nego što otpočne glasanje; nadležni organ će se uvjeriti da je e-sistem glasanja originalan i funkcioniše ispravno; samo lice imenovano od strane izborne komisije ima pristup centralnoj infrastrukturi, serveru i izvoru podataka, tajnost glasanja se mora čuvati i do prebrojavanja glasovi moraju biti zapečaćeni; ukoliko se glasovi skladište ili transportuju u spoljno okruženje, oni moraju biti šifrovani (kriptovani);

2.3 Operativni standardi

Operativni standardi su podijeljeni u šest djelova i odnose se na različite kategorije:

Obavještenja - izborna komisija obavještava glasače o rasporedu svih faza e-glasanja; e-glasanje ne može početi prije obavještenja o e-glasanju; glasači moraju biti obavješteni znatno prije e-glasanja o načinu organizacije e-glasanja.

Birači - mora postojati glasački spisak koji se redovno ažuriran, a glasačima se mora omogućnosti da provjere informacije koje se u registru vode o njima; ukoliko postoji mogućnosti, kreirati elektronski glasački spisak i omogućiti onlajn registraciju glasača.

Kandidati - dati mogućnost da se kandidatura za izbore vrši i preko interneta; lista kandidata sa interneta, osim na internetu napraviti dostupnu javnosti i na druge načine.

Glasanje - posebno je važno onemogućiti duplo glasanje u slučaju kada je istovremeno omogućeno glasanje sa udaljenih lokacija (npr. glasanje iz inostranstva putem interneta) i glasanje na glasačkim mjestima; e-glasanje sa udaljenih lokacija može da počne ili da se završi prije otvaranja glasačkih mjesta; glasačima će biti dostupna podrška i vodič kroz proceduru; glasačima je potrebno objasniti na koje sve načine mogu da iskoriste pravo da glasaju, pri čemu treba obratiti pažnju da se ni jedan od načina ne favorizuje; sistem ne smije da sadrži poruke koje mogu da utiču na izbor glasača; prije nego glasač pristupi e-glasanju mora biti jasno upozoren da se ne radi o probnom nego pravom e-glasanju; informacije o glasanju glasača nestaće sa ekrana odmah nakon glasanja.

Rezultati glasanja - elektronski sistem neće dozvoliti prebrojavanje glasova prije zatvaranja glasačkih kutija, a ove informacije biće dostupne javnosti tek nakon završetka perioda predviđenog za glasanje; elektronski informacioni sistem će spriječiti

obradu informacija koja može da ukaže na kojoj opciji je pojedinac u nekoj izbornoj jedinici dao glas; dekripcija neophodna za prebrojavanje glasova vrši se što je prije moguće nakon zatvaranja glasačkih mjesta; prilikom prebrojavanja glasova biće omogućeno učešće nadležnih izbornih organa i posmatrača; zapisnik o prebrojavanju elektronskih glasova, koji uključuje informacije o početku i završetku glasanja, čuva se.

Kontrola glasanja - sistem elektronskog glasanja mora biti kontrolisan; zaključci dobijeni na osnovu elektronskog glasanja će se primjenjivati u budućnosti na elektronskim glasanjima i elektronskim referendumima.

Glava 3

Proces glasanja

U cilju pojednostavljenja analize, predstavićemo zajednički referentni model koji sadrži bitne karakteristike sistema glasanja. Sistem se sastoji iz dvije cjeline i to glasačkog mjesta i izbornog centara.

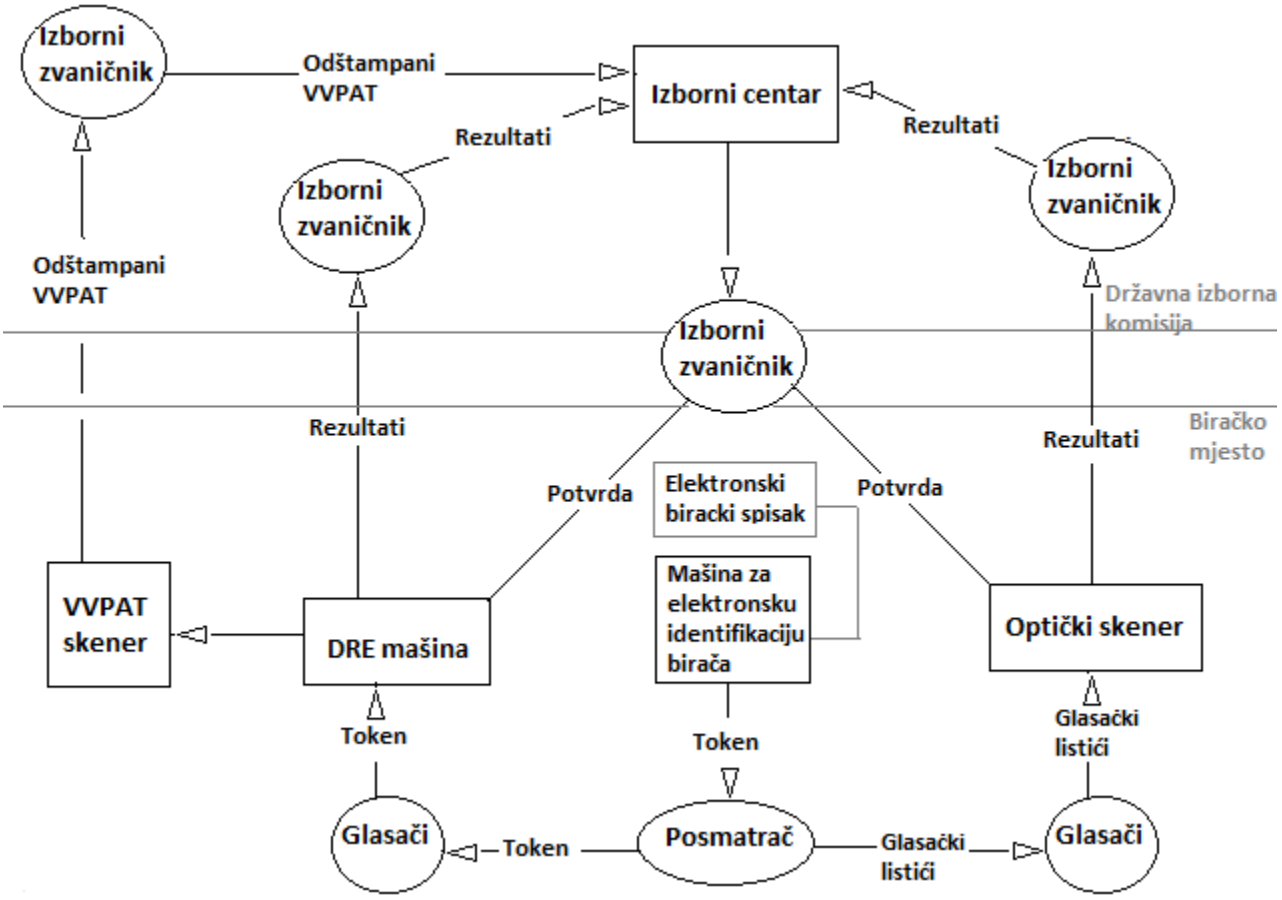
Na glasačkom mjestu se nalaze:

1. Izborna komisija;
2. Birački spiskovi;
3. DRE (direct-recording electronic) - uređaji za elektronsko glasanje. DRE mašine su priključene na uređaj koji štampa potvrdu kada glasač završi glasanje - VVPAT štampač (Voter-verified paper audit trail);
4. Optički skeneri glasačkih listića.

U izbornim centrima se nalaze:

1. Izborna komisija;
2. Brzi optički skener glasačkih listića;

Izbori se mogu posmatrati u tri odvojene faze i to: faza prije glasanja, faza glasanja i faza poslije glasanja.



Slika 3.1: Primjer jednog glasačkog mjesta.

3.1 Faza prije glasanja

U fazi prije glasanja, potrebno je:

1. Definisati koja vrsta izbora je u pitanju;
2. Odštampati glasačke listiće koji se koriste za optički sistem;
3. Podesiti glasačke aparate;
4. Identifikovati glasače na svakom glasačkom mjestu;
5. Podijeliti glasačku opremu i glasačke spiskove na svim glasačkim mjestima;

U zavisnosti od proizvođača izbornih mašina postoje određene varijacije istih, više u smislu detalja nego u njihovim generalnim funkcionalnostima. Izborna komisija svake države zahtijeva od proizvođača određena prilagođavanja mašina. Ovo se najčešće radi zbog specifičnosti koje se mogu pojaviti u izbornom zakonu. Nakon što je brojač glasova u mašinama resetovan, i satovi podešeni na odgovarajuće vrijeme tek tada se mašine dostavljaju na glasačka mjesta. Fajlovi za glasanje moraju biti zaštićeni od ometanja, a memorijske kartice dostavljene sa nekim fizičkim mjerama sigurnosti, zapečaćene u opremi za glasanje ili u zatvorenoj ambalaži. Kada se memorije jednom instaliraju na mašine, mogu se ukloniti samo tako što će se odsjeći. Ovakve fizičke zaštite omogućavaju članovima izborne komisije da provjere da nije došlo do zloupotreba mašine, odnosno podmetanja podataka.

3.2 Faza glasanja

Kada se otvore glasačka mjesta, glasanje može da počne. Tačni detalji ove faze zavise od zakonskih okvira i procedura, tehnologije i proizvođača opreme, ali u okviru date tehnologije postoje opšta pravila za proizvođače.[**?**]

Kao i kod dosadašnjeg načina glasanja, glasači se prvo *identifikuju*. Identifikacija se najčešće vrši očitavanjem podataka sa elektronske lične karte. U DRE sistemima, izborna komisija na glasačkom mjestu identifikuje glasača i koristi štampač za izdavanje potvrde, sa kojom glasač može glasati. Sa potvrdom glasač dolazi do optičkog skenera. On očitava potvrdu i ukoliko je validna, na DRE mašini će se dozvoliti glasaču da glasa. Ovaj dio e-glasanja se zove sistem za *identifikaciju glasača*.

Jednom kada je mašina dobila potvrdu da glasač ima pravo glasa, ona se aktivira i provodi glasača kroz svaki korak i dozvoljava mu da izabere kandidata. DRE mašine omogućavaju elektronsko glasanje koje je se razlikuje od dosadašnjeg načina

glasanja. Glasaču se na ekranu DRE mašine pojavljuje glasački listić. Glasač umjesto zaokruživanja rednog broja kandidata kako se to radilo na papirnom glasačkom listiću, pritiskom tastera sa rednim brojem kandidata vrši glasanje. Prije nego što glasač potvrdi svoje glasanje, rezultat glasanja je predstavljen na ekranu. Glasaču je data mogućnost da preispita svoj izbor, i u slučaju da je pogriješio glasaču je data mogućnost ispravke. Nakon potvrde od strane glasača da stvarno želi izbor koji je načinio, glas se čuva. Jednom kada glasač izvrši glasanje, DRE mašina zapamti glas.

U toku dana svaki od glasova se bilježi u bazi ili fajlu na DRE mašini. Na kraju dana, svi ovi fajlovi mogu biti iznešeni iz DRE mašine na memorijskoj kartici, ili se mogu transportovati mrežom ako postoji, do centralne izborne komisije. DRE mašine automatski uklanjaju višak na glasačkim listićima, ali i prazne listiće, tako da nije moguće napraviti nevažeće listiće. U svakom slučaju, izborna komisija će sakupiti fajlove sa svakog glasačkog mjesta, objediniti ih i objaviti u vidu izvještaja.

Svaka DRE mašina posjeduje *VVPAT štampač* koji štampa potvrdu po završetku glasanja jednog glasača. Jednom kada glasač potvrdi ili poništi glasački listić, odgovarajuća indikacija se odštampa na VVPAT kontrolnoj traci. Kada glasač izvrši glasanje, VVPAT kontrolna traka se uvija tako da nije vidna (tj. glas se prihvata i čuva). Funkcija kontolnog VVPAT štampača je da spriječi zloupotrebu, u smislu dodavanja papira ili slikanja rezultata glasanja. Svaki glas koji se čuva na VVPAT kontrolnoj traci je štampana kopija svakog zapisa u fajlu koji se kreira po glasanju.

Postoje dva modela za razmještanje opreme na glasačkim mjestima. U DRE modelima, svako glasačko mjesto posjeduje određen broj DRE mašina i isti broj optičkih skenera za potvrde. Mašina i skener se nalaze u glasačkoj kabini. U hibridnim modelima, svako glasačko mjesto posjeduje jedan optički skener i jednu ili više DRE mašina. U izbornoj kabini se nalazi samo DRE mašina, a optički skener je zajednički za više glasačkih kabina.

3.3 Faza poslije glasanja

Nakon što se izbori završe, izborna komisija treba da uradi sljedeće:

1. Dokumentuje neprebrojane i neiskorišćene listiće;
2. Potvrdi poklapanje broja glasačkih listića za svaku bazu, dobijenih od pojedinačnih glasačkih mjesta, sa svim prebrojanim listićima;
3. Da predstavi konačni rezultat;

Prve dvije nabrojane aktivnosti su prilično jednostavne. Važno je istaći da se drugi korak odnosi na elektronsko glasanje. Rezultati se šalju na memorijsku karticu.

Kod e-glasanja proces prebrojavanja glasova vrši VVPAT traka. Ukoliko nije bilo nepravilnosti, podaci sa VVPAT trake (kontrolne trake) će se poklapiti sa podacima u DRE mašinama.

Glava 4

Bingo šema za elektronsko glasanje

Bingo šema za glasanje, koju ćemo opisati, dobila je ime zbog svoje sličnosti sa izvlačenjem kuglice iz bingo bubnja. Ova šema generiše *slučajan broj* iz zadatog skupa, isto kao što se i u bingo izvlačenju vadi na slučajan način kuglica iz bingo bubnja iz skupa kuglica koji je ograničen i numerisan. Kao i prilikom izvlačenja kuglice na bingu i u ovoj šemi postoji tzv. semafor na kojem se vidi koji su brojevi do tada izvučeni, odnosno generisani. Osim osobina navedenih kao preporuke Savjeta Evrope u prvom dijelu rada, ova šema omogućava i sljedeće:

1. Da glasač provjeri da li je stvarno njegov glas prihvaćen i brojan kandidatu kojem je namijenjen;

2. Da svako provjeri da li su glasovi ispravno prebrojani, a bez da zna ko je za koga glasao (Zero-knowledge proof);

3. Da se postigne apsolutna sigurnost i neograničena tajnost glasanja. Pod neograničenom tajnošću glasanja podrazumijeva se da za bilo koji vremenski interval od završetka izbora niko ne može saznati kako je neki pojedinac glasao;

4. Da se glas ne može prodati tj. glasač ne može potvrditi da je glasao za odeđenog kandidata, niti da bilo ko drugi može doći do sadržaja glasačkog listića;

U bingo algoritmu generišemo dva tipa slučajnih brojeva. Slučajne brojeve generišemo korišćenjem generatora slučajnih brojeva. Jedan tip slučajnih brojeva su *lažni slučajni brojevi* koje generišemo prije glasanja, a drugi tip su *slučajni brojevi koji se generišu u trenutku odabira kandidata.* Oba tipa slučajnih brojeva su detaljnije opisana u sljedećem poglavlju. Anonimnost prilikom glasanja i jednako pravo glasa se, za razliku od e-glasanja, postižu tradicionalnim metodama. Izborna komisija, na glasačkom mjestu, vrši provjeru da li je glasač iskoristio pravo glasa, i ukoliko nije dozvoljava mu da glasa.

Bingo šema je vrlo upotrebljiva. Glasaču nije neophodna kompjuterska pismenost niti razumijevanje algoritama, koji se nalaze u pozadini, da bi mogao da koristi sve opcije koje šema pruža. Glasanje se vrši korišćenjem mašine za elektronsko glasanje. Glasač vrši odabir kandidata pritiskom na dugme koje je vezano za određenog kandidata. Da bi provjerio da li je njegov glas uvažen, glasaču je dovoljno da provjeri da li su dva *slučajna broja* ista i da li je njegov glasački broj objavljen na glasačkom semaforu. Za provjeru pojedinačnih glasova nije potrebno da se svi glasovi provjeravaju. Zapravo, bilo koji glasač koji hoće da provjeri svoj glas to može uraditi i ako niko prije njega nije vršio provjeru.

4.1 Pomoćni algoritmi Bingo šeme

Pretpostavke koje definišu sigurnost Bingo šeme, a koje smo naveli u uvodnom poglavlju, realizuju se uz pomoć sledećih algoritama:

1. Komitment šema;
2. Generator slučajnih brojeva;
3. Unošenje šumova (Generisanje lažnih brojeva);

4.1.1 Komitment šeme

Komitment šeme, poznate u kriptografiji, dozvoljavaju jednoj strani da izabere određenu vrijednost, na način da samo ta strana zna tu vrijednost, sa mogućnošću da je naknadno otkrije i potvrdi. One su napravljene tako da se odabir koji je izvršen na početku ne može promijeniti. Komitment šeme imaju značajnu primjenu u kriptografskim protokolima.

Pojednostavljeno govoreći, komitment šemu opisujemo: pošiljalac šalje poruku, istu stavlja u kutiju, zaključava je i daje je primaocu. Poruka je sakrivena od primaoca i ne može se otključati bez pomoći pošiljaoca. Sve dok primalac ima kutiju, poruka se ne može promijeniti dok pošiljalac to ne dozvoli.

Interakcija kod komitment algoritma sastoji se iz dva dijela:

1. *Komitment faza* u kojoj se vrijednosti biraju i izračunavaju. U jednostavnim protoklima, komit faza sastoji se od poruke koju pošiljalac šalje primaocu. Ta poruka se naziva ***komitment*** i komitment se dalje šalje primaocu.

   Komitment C za vrijednost x i za slučajnu vrijednosti r se računa na sledeći način:

   $$C = Commit(x, r)$$

2. *Faza otkrivanja* je faza u kojoj se vrijednosti otkrivaju i potvrđuju. Ova faza se sastoji od komitmenta, koju pošiljalac otvara primaocu. Vrijednost izabrana u ovoj fazi mora biti jedina koju pošiljalac može da računa i potvrdi. Ovo svojstvo se naziva ***bajding svojstvo***. Svojstvo komitment algoritma da se sadržaj poruke ne može otkriti od strane primaoca sve dok pošiljalac to ne omogući naziva se ***hajding svojstvo***.

   $$CheckReveal(C, x, r)$$

je potvrda da je su za računanje C korišćene vrijednosti x i r.

Kod bingo šeme za *Commit* funkciju se koristi diskretni logaritamski komitment poznatiji kao *Pedersenov komitment*.

4.1.2 Pedersenov komitment algoritam

Javni ključevi pošiljaoca i primaoca su iz ciklične grupe G prostog reda q, u kojoj je je diskretni logaritamski problem težak. Kod Pedersenovog komitment algoritma ne koristimo jednu slučajnu vrijednost već dvije slučajne vrijednosti $m \in \{1, ..., q\}$ i $r \in \{1, ..., q\}$, gdje je q veliki prost broj. Biraju se dva generatora $g, h \in G$, na slučajan način, tako da je diskretni logaritamski problem g za bazu h nepoznat. Da bi se izvršio komitmnet vrijednosti $m \in \{1, ..., q\}$ pošiljalac bira slučajnu vrijednost $r \in \{1, ..., q\}$ i računa komitment na sledeći način

$$c = g^m h^r.$$

Za potvrđivanje komitmenta pošiljalac mora da pošalje par (m, r) i tek tada primalac može da provjeri da li je $c = g^m h^r$.

4.1.3 Generator slučajnih brojeva

Idealni generatori slučajnih brojeva crpe svoju 'slučajnost' iz događaja iz prirode. Pošto bi idealan generator zahtijevao veliku infrastrukturu, nama ne bi bio pogodan za implementaciju u okviru Bingo šeme koja se koristi za elektronsko glasanje. Zbog toga se najčešće, umjesto generatora slučajnih brojeva koriste generatori pseudo-slučajnih brojeva.

Jedan od najpopularnijih generatora pseudo-slučajnih brojeva koji se i danas koristi je *linearni generator slučajnih brojeva.* Američki matematičar Derrick Henry Lehmer je 1948. godine konstruisao ovaj generator.

Vrlo često se koristi kao osnovni element nekih naprednijih generatora. Samim tim, razumijevanje principa rada i osnovnih osobina osnivih generatora je neophodno za projekovanje drugih, „boljih“ generatora.

U implementaciji linearnog generatora potrebno je odrediti 4 parametra: *modul* m, koeficijetnt a, inkrement c i početnu vrednost X_0. Niz slučajnih brojeva dobija se korišćenjem izraza:

$$X_{n+1} \equiv aX_n + c \pmod{m}$$

Izbor parametara nije trivijalan zadatak. Na primer, ukoliko izaberemo $m = 10, a = c = X_0 = 7$, dobijena sekvenca će biti: 7, 6, 9, 0, 7, 6, 9, 0... Sekvenca koju generiše ovako odabran linearni generator slučajnih brojeva ima svojstvo cikličnog ponavljanja. Međutim, ovo je osobina svih pseudo-slučajnih generatora. Potrebno je obezbijediti da generator ima što dužu ciklični period, a što se postiže izborom velikog broja m. U našem slučaju nije teško odabrati dovoljno veliko m, ya unaprijed poznat broj glasača.

Kako je slučajni broj X_i određen svojim prethodnikom X_{i-1} i kako postoji ukupno m različitih mogućih vrednosti za X_i, maksimalan period, odnosno dužina ciklusa linearnog generatora slučajnih brojeva je m. U vrijeme kada računari nisu bili toliko moćni kao danas, izbor modula je obično bio neki stepen broja 2. Tako se dobijao brz generator koji je možda bio brži, ali generisani brojevi su u binarnoj reprezentaciji imali vrlo predvidljiv šablon, pa je tako najmanje značajni bit imao period ne veći od 1, drugi nije imao period ne veći od 2, a treći ne veći od 4 itd. U nekim primjenama ovog generatora, bitovi nižeg reda nisu toliko značajni i izbor ovakvog modula će

proizvesti zadovoljavajuće rezultate. Slični, predvidljivi šabloni se javljaju i kada je modul djeljiv nekim malim prostim brojem.

Izbor množitelja je takođe bitan za postizanje maksimalne dužine perioda za izabrano m. Na primjer, možemo izabrati sledeće parametre: $a = c = 1$ i tada bi formula za računanje sledećeg broja bila jednostavna, čime bi se očigledno postigao period dužine m, ali generisani brojevi ne bi čak ni izgledali nasumično. Donald E. Knuth formulisao je i dokazao teoremu koja se tiče izbora parametara kod linearnog generatora slučajnih brojeva i obezbjeđuje maksimalnu dužinu perioda. [5]

Teorema 1. *Parametri linearnog generatora slučajnih brojeva se biraju na sledeći način:*

1. *c i m ne smiju imati zajedničke proste djelioce;*
2. *Ako je q neki prost broj koji dijeli m, on takođe dijeli i $b = a - 1$;*
3. *Ako je m dijeljivo sa 4, onda i $b = a - 1$ mora biti dijeljivo sa 4;*

Dokaz teoreme se dobija kao direktna posledica sledećih lema.

Lema 1. *Neka je p prost broj, i neka je e pozitivni cijeli broj tako da je $p^e > 2$. Ako*

$$x \equiv 1 \pmod{p^e}, \quad x \not\equiv 1 \pmod{p^{e+1}}$$

tada je

$$x^p \equiv 1 \pmod{p^{e+1}}, \quad x^p \not\equiv 1 \pmod{p^{e+2}}$$

Lema 2. *Neka je m dato kao proizvod:*

$$m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

Dužina linearnog generatora λ određena sa (X_0, a, c, m) je najmanji zajednički djelilac dužine λ_j za period linearnog generatora

$$(X_0 \bmod p_j^{e_j}, a \bmod p_j^{e_j}, c \bmod p_j^{e_j}, p_j^{e_j}),\ 1 \leq j \leq t$$

Lema 3. *Pretpostavimo da je $1 < a < p^e$ gdje je p prost broj. Ako je λ najmanji pozitivni cijeli broj za koji je $(\frac{a^\lambda}{a-1}) \equiv 0 \pmod{p^e}$, tada*

$$\lambda = p^e \quad \Leftrightarrow \quad \begin{cases} a \equiv 1 \pmod{p} \ \textit{kada je } p > 2 \\ a \equiv 1 \pmod{4} \ \textit{kada je } p = 2 \end{cases}$$

Na primjer, ako izaberemo parametre u skladu sa teoremom: $X_0 = 7, a = 13$, $c = 5, m = 18$, period će biti maksimalne dužine od od 18 brojeva: 7, 6, 11, 4, 3, 8, 1, 0, 5, 16, 15, 2, 13, 12, 17, 19, 9, 14, 7, 6, 11, 4, ... Odabir parametara je u skladu sa navedenom teoremom, jer je:

1. $\mathbf{nzd}(5, 18) = 1$
2. $13 \equiv 1 \pmod{3}$ jer su 2, 3 prosti dijelioci broja 18.
3. m nije djeljivo sa 4

Izbor parametara, kao i izbor same funkcije koja će generisati pseudo-slučajne brojeve mora biti pažljiv. Ispitivanja su pokazala da generatori koji koriste nasumično odabrane funkcije čije ponašanje nije dovoljno ispitano zapravo daju veoma loše rezultate.

4.1.4 Lažni brojevi

Bingo šema za elektronsko glasanje koristi lažne brojeve kao glavno sredstvo da bi osigurala glasaču da je njegov glas pridružen željenom kandidatu.Posmatrajmo izbore sa v glasača i k kandidata i naravno, jedan glas za svakog glasača. Bingo šema zahtjeva da se svakom kandidatu generiše oniliko lažnih brojeva koliko je i glasača ili više. Za svakog kandidata K_i generiše se lažan broj L_{ji} pri čemu $j \in \{1, ..., v\}$. Za svaki par (K_i, L_{ji}) dodjeljuje se slučajan broj r_{ji} i pravi komitment

$$(commit(r_{ji}), commit(K_i)) = (g^{r_{ji}} h^{f(r_{ji})}, g^{K_i} h^{f(K_i)}),$$

gdje je f neka funkcija. Ovako napravljeni komitmenti se objavljuju u fazi prije izbora kao dokaz da je svaki kandidat dobio isti broj lažnih glasova. Da bi se ostvarila regularnost ovog protokola potrebno je da se generiše isti broj lažnih brojeva za svakog kandidata.

4.2 Koncept Bingo šeme

Ideja Bingo šeme se zasniva na generisanju slučajnih brojeva. Potrebno je generisati dvije grupe slučajnih brojeva i to *lažni slučajni brojevi* koji se generišu prije izbora i *svježi slučajni brojevi* koji se generišu u trenutku odabira kandidata. Prije nego izbori zvanično počnu potrebno je generisati jednak broj lažnih brojeva za svakog kandidata. Taj broj može biti veći ili jednak broju upisanih glasača. Komitmenti lažnih brojeva su javni.

U glasačkoj kabini se nalazi generator svježih slučajnih brojeva koji generiše slučajan broj u trenutku odabira kandidata i prikazuje ga na ekranu. Taj broj je vidljiv samo za glasača i nakon što glasač potvdi svoj glas, nestaje sa ekrana. Po završetku

glasanja, štampa se potvrda koja je zapravo lista slučajnih brojeva. Na toj potvrdi su svi brojevi lažni, osim onog pored kandidata za kojeg se opredijelio glasač.

U toku izbornog procesa, redom se objavljuju sve potvrde na oglasnoj tabli, tako da svaki glasač može da utvrdi da je njegov glas prihvaćen onako kako je želio.

Na kraju izbornog dana, objavljuju se svi neiskorišćeni lažni brojevi i na taj način se daje sigurnost da se nije mogla desiti manipulacija sa slučajnim brojevima. U nastavku rada opisaćemo svaku fazu glasanja pojedinačno.

Slika 4.1: Prikaz DRE mašine, generatora slučajnih brojeva i potvrde u trenutku glasanja.

Da bi olakšali opis šeme ograničavamo se na jednu glasačku mašinu, s napomenom da je proširenje na više mašina takođe jednostavno. U glasačkoj kabini se nalazi generator slučajnih brojeva (RNG) i glasačka mašina. [4]

4.2.1 Faza prije glasanja

Izborni zvaničnici u ovoj fazi moraju dati dokaz da se generisao jednak broj lažnih glasova za svakog kandidata. Taj dokaz predstavljaju komitmenti lažnih brojeva. Oni se objavljuju na oglasnoj tabli i samim tim svako može da ih provjeri.

4.2.2 Faza glasanja

Da bi se izvršilo glasanje, u glasačkoj kabini se vrše sljedeći koraci::

1. Glasač vrši odabir kandidata pritiskom na dugme koje je vezano za određenog kandidata;

2. Generator slučajnih brojeva generiše novi slučajni broj R;

3. Slučajni broj R se prenosi na glasačku mašinu i dodjeljuje kandidatu kojeg je glasač izabrao. Za svakog drugog kandidata, mašina će izvući slučajno jedan broj iz grupe lažnih brojeva za odgovarajućeg kandidata. Nakon toga mašina će odštampati listu sa kandidatima i brojevima. Kandidatu kojeg je glasač odabrao biće dodijeljen novi broj R, dok će ostalim kandidatima biti dodijeljeni slučajni brojevi iz grupe lažnih brojeva;

4. Glasač sam utvrđuje da je broj R koji je generisan u trenutku kada je glasač glasao upravo taj broj koji je dodijeljen kandidatu kojeg je izabrao

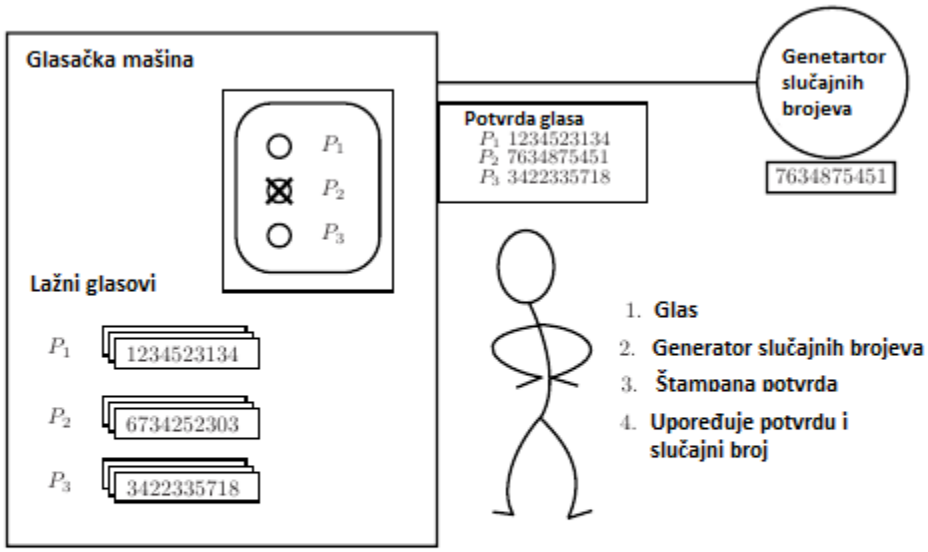
5. Glasač napušta kabinu i uzima potvrdu. Treće lice ne može utvrditi koji od brojeva je iz grupe lažnih ;

4.2.3 Faza poslije glasanja

Nakon završetka procesa glasanja glasačka mašina broji rezultate i šalje ih zajedno sa dokazom o ispravnosti na glavnu oglasnu tablu. Objavljeni podaci se sastoje od četiri dijela:

1. Krajnji rezultat glasanja;

2. Leksikografski sortirana lista svih izdatih potvrda;



Slika 4.2: Opis glasačkog listića .

3. Lista svih neiskorišćenih lažnih brojeva se takođe objavljuje na oglasnoj tabli;

4. Neinterakivni zero-knowledge dokaz za ispravnost tj. da je lažni broj svakog neiskorišćenog komitmenta, iskorišćen na jednoj potvrdi.

Sada svaki glasač može lako da provjeri da je njegova potvrda uključena u listi i da je samim tim izbrojana. Lista neiskorišćenih lažnih glasova se objevljuje tako da se uz odgovarajući komitment, koji je generisan u fazi prije izbora, objavljuje i slučajan broj r_{ji} tako da svako može da provjeri da je taj komitment takođe objavljen i u fazi prije glasanja. Na kraju izbornog dana lako se može utvrditi da su svi neiskorišćeni komitmenti prikazani jer su nam sada svi parametri poznati.

4.2.4 Verifikacija izbornog procesa

U Bingo šemi verifikacija izbornog procesa se može podijeliti na dva dijela:

1. Individualna verifikacija;

2. Globalna verifikacija;

Individualnu verifikaciju obavlja sam glasač. Ona se sastoji iz dva koraka. U toku izbora, glasač provjerava da li je njegov glas ispravno odštampan na potvrdi. Takođe, provjerava da li je njegov glas dodijeljen onome kome je namijenjen. To se postiže na način što glasač provjerava da li je slučajni broj koji je generisan u toku glasanja, i prikazan na ekranu, odštampan pored kandidata za kojeg je glasao. Ovo je akcija koja se odvija unutar glasačke kabine. [3]
U drugom koraku glasač može da provjeri da li je njegov glas brojan. U ovom koraku on provjerava da li je njegova potvrda objavljena na oglasnoj tabli. Oglasnu tablu nije nužno fizički postaviti na glasačkom mjestu, već se podaci mogu predstaviti tabelarno i objaviti na zvaničnoj internet stranici Izborne Komisije.

Globalna verifikacija zahtijeva od glasačke komisije da dokaže sljedeće:

1. Da svaki kandidat ima isti broj lažnih brojeva koji se generišu u fazi prije izbora i da svaki komitment za lažne glasove objavi;

2. Da svaka potvrda ne sadrži više od jednog pravog glasa za svakog kandidata;

3. Da je svaki lažni broj iskorišćen, bilo da je odštampan na potvrdi ili se objavio na kraju izbornog dana sa ostalima neiskorišćenim brojevima. Kada se objave neiskorišćeni lažni glasovi tada se objavljuju i slučajni brojevi r_{ji} tako da se može utvrditi za svaki broj da se nalazio i objavio u fazi prije izbora. Samim

tim se vrši verifikacija da je za svakog kandidata generisan jednak broj lažnih brojeva;

4. Da su poklapanja u generisanju slučajnih brojeva, ako postoje, statistički zanemarljiva.

Glava 5

Ciljevi napadača

Na najvišem nivou, napadači mogu imati jedan od ili kombinaciju više ciljeva: predstavljanje netačnog broj glasova, uskraćivanje nekim ili svim glasačima mogućnost glasanja, odlaganje saznanja rezultata izbora, kršenje tajnosti glasanja.

5.1 Predstavljanje netačnog broj glasova

Predstavljanje netačnog broja glasova je najočigledniji napad na sistem glasanja. Postoje različiti načini da se utiče na broj glasova:

1. Zbunjivanje glasača sa ciljem da glasaju drugačije od njihove namjere;
2. Izmjena glasova, u kompjuteru, prije nego što su sačuvani;
3. Izmjena glasova u medijumu za čuvanje glasova, nakon što su prvobitno sačuvani.

5.2 Uskraćivanje mogućnosti glasanja

Dvije klasične tehnike kojima se utiče na izborni rezultat, bez obzira na način glasanja, su uticaj na glasače ili suzbijanje glasanja. Napadači mogu da spriječe glasanje na način što će uticati na određenu grupu glasača. Napadač može da:

1. Onemogući rad određenih mašina;

2. Programira selektivno kvarove mašina pri pokušaju glasanja određene opcije;

3. Uspori rad određenog broja, ili svih mašina, sa ciljem da se produži vrijeme glasanja 10-15 sekundi i na taj način formiraju veliki redovi.

5.3 Odlaganje saznanja rezultata glasanja

Često je dovoljno da napadač osujeti izborni proces i na taj način ispuni svoje ciljeve. Napadač može da odloži saznanje rezultata izbora na način što će:

1. Učiniti glasačku opremu privremeno nedostunom ili neupotrebljivom (Razbijanje intjerfejsa DRE mašina, potrošiti papir u VVPAT štampaču);

2. Odložiti isporuku glasova uređajima za evidenciju istih.

5.4 Kršenje tajnosti glasanja

Napadač koji ne može da utiče na glasanje direktno može biti u mogućnosti da utiče kako će neki pojedinac ili grupa ljudi glasati. Neki od načina da se utiče na tajnost glasanja su sljedeći:

1. Kupovina glasova/ubjeđivanje glasača;

2. Sakupljanje informacija;

Pri pokušaju kupovine i ubjeđivanja glasača, napadač plaća ili vrši pritisak na glasače da glasaju na određen način. Da bi takav napad bio uspješan, napadač mora biti u mogućnosti da provjeri da li je glasač glasao upravo onako kako mu je i naređeno

odnosno plaćeno. Upotreba Bingo šeme za elektronsko glasanje čini da navedeni pokušaji kupovine glasova glasača budu neatraktivni. Iako se svi komitmenti lažnih brojeva objavljuju prije izbora napadač ne može da utvrdi koji je broj sa potvrde koju glasač posjduje lažan a koji je svježe generisan.

Glava 6

Potencijalni napadači

6.1 Napadači koji nemaju pristup opremi za elektronsko glasanje

Autsajder - nema nikakav pristup sistemu za glasanje, odnosno opremi. Mogu biti u potpunosti izvan glasačkog sistema ili fizički prisutni (kao posmatrači), ali bez mogućnosti da fizički dotaknu opremu. Takav napadač ima ograničenu sposobnost u kontekstu ove analize.

Pošto su mašine za elektronsko glasanje povezane sa spoljnim svijetom (posredstvom interneta ili povezane sa nekim drugim mašinama koje su prikopčane na neku mrežu) napadač može pokušati da promijeni softver koji upravlja cjelokupnim izbornim sistemom ili jednim glasačkim mjestom. Nakon toga, pojedinci bi dobili mogućnost da napadnu sistem glasanja iz bilo kojeg dijela svijeta.

Takođe, ako glasačka mjesta nemaju dovoljnu zaštitu uoči glasanja, autsajderi mogu fizički oštetiti opremu za glasanje.

6.2 Napadači koji imaju pristup opremi za elektronsko glasanje

Glasači - takođe mogu biti potencijalni napadači. Zbog prirode izbora, potrebe da se glasačima omogući sloboda i tajnost izbora, glasačima se mora omogućiti pristup DRE mašini bez nadzora, na određeno vrijeme. Zlonamjerni glasači mogu pravo glasa, koje im zakon obezbjeđuje, iskoristiti za opstruiranje izbora ili procesa glasanjana na različite načine. Šteta se može ogledati u vandalizaciji DRE mašine za glasanje ili u kršenju tajnosti glasanja, slikanjem svog izbora.

Posmatrači - za razliku od glasača, posmatrači u okviru svojih ovlašćenja imaju mogućnosi dužeg pristupa DRE mašinama za glasanje, a time i veće mogućnosti za remećenje regularnosti izbora kroz onesposobljavanje opreme.

Posmatrači koji su u dosluhu jedni sa drugim predstavljaju još jedan problem. Ako glasačko mjesto ima više od jednog posmatrača-napadača, oni mogu da zaobiđu mnoge od procedura namijenjenih za otkrivanje problema ili zloupotrijebe ili izmanipulišu izbornu opremu. U ekstremnom slučaju, ako bi svi posmatrači glasačkog mjesta zajedno imali loše namjere, onda bi imali slobodu da ignorišu mnoge procedure i na taj način izvrše prevaru sa manjim mogućnostima da budu otkriveni. Treba napomenuti da su posmatrači većinom volonteri i da su podvrgnuti vrlo slaboj provjeri, ako se uopšte i provjeravaju.

Izborni zvaničnici - Za razliku od posmatrača izborni zvaničnici imaju četiri značajne mogućnosti:

1. Pristup funkcionalnosti lokalne glasačke opreme koji može biti zabranjen posmatračima;

2. Pristup velikom broju glasačke opreme između izbora;

3. Pristup pozadinskom izbornom sistemu upravljanja koji se koristi za upravljanje opremom;

4. Kreiranje glasačkih listića i tabelarnih prikaza;

Treća navedena mogućnost je u potpunosti nedostupna posmatračima. Pozadinski izborni upravljački sistemi rade na generalnim kompjuterima koje koriste izborni zvaničnici. Ako su ti sistemi kompromitovani mogu se koristiti za malverzacije sa izbornom opremom glasačkog mjesta, pravljenje lažnih ili netačnih listića, kao i za nepravilno brojanje glasova. Napad od strane izbornih zvaničnika se može ostvariti na tri načina. Prvi, napadač može koristiti legitiman pristup da pokrene napad. Software može dati priliku izbornom zvaničniku da napravi "korekcije" glasova. Te "korekcije"mogu biti netačne. Drugo, izborni zvaničnik možda nađe način kako da savlada tehnički pristup kontrolama u softveru upravljačkog sistema izbora i da kompromituje podatke o glasovima. Treće, zvaničnik bi mogao da direktno kompromituje kompjutere koji sadrže softver za glasanje. Tačno je da, ako napadač ima fizički pristup opštim računarima, on na kraju može da preuzme kontrolu nad njima. Ovo se može postići na više načina, od napada na softver do direktnog ugrožavanja hardvera.

Zaposleni kod proizvođača opreme - konačno, razmatramo napadače koji su zaposleni u službi proizvođača opreme. Takvi napadači se mogu podijeliti u dvije kategorije: oni koji su uključeni u proizvodnju hardvera i softvera prije izbora, i onih koji su prisutni na glasačkom mjestu ili izbornom centralnom magacinu tokom izbora. Napadač zaposlen kod proizvođača opreme može pripadati bilo kojoj od navedenih kategorija.

Napadač koji učestvuje u razvoju i izradi softvera i hardvera za izborni sistem ima veliku mogućnost za kompromitovanje sistema. Napadač može, na primjer, namjerno da instalira maliciozni kod u softver izbora, instalira zloupotrebljive ranjivosti

ili bek-dor u sistemu, ili namjerno dizajniraju hardvare na takav način da ga je lako kompromitovati. Takve napade je teško detektovati iz razloga što mogu proći kao obične greške, jer je njihovo prisustvo često i u velikim softver projektima. Treba imati na umu, da za uspješnost takvog napada nije važno da li je softver sertifikovan ili ne.

Zaposleni kod prodavača mašina takođe može da asistira izbornom zvaničniku ili posmatraču. Na primjer, zaposleni može biti prisutan u izbornom centru tokom ili posle glasanja da pomogne izbornim zvaničnicima, odogvarajući na pitanja ili da popravlja pokvarenu opremu. Zaposleni kod proizvođača opreme takođe može biti prisutan u izbornom centru da pomogne prilikom instalacije i upravljanja glasačkog sistema ili da obučava posmatrače i ostalo osoblje. Takav napadač će imati isti pristup opremi kao posmatrač ili izborni zvaničnik, ali će imati značajnu slobodu kretanja. Dužnost im je da popravljaju greške i da instaliraju softver, aktivnosti kojima se može kompromitovati oprema su manje primjetne. U onoj mjeri u kojoj sistemi imaju skrivene administrativne interfejse, vjerovatno bi imali pristup i njima.

Glava 7

Zaključak

Bingo šema koja je opisana u radu je vrlo primjenjiva i korisna je za poboljšanje sigurnosti procesa glasanja. Takođe, za njenu implementaciju potrebno je osigurati određenu infrastrukturu. Finansijski faktor bi mogao biti prepreka da se ova šema koristi. Ukoliko postoji infrastruktura za elektronsko glasanje, sistem za elektronsku identifikaciju, DRE mašine i VVPAT štampače, Bingo šema se lako implementira. Za proširenje elektronskog glasanja do elektronskog glasanja sa Bingo šemom bilo bi potrebno još dodati generator slučajnog broja u glasačkoj kabini, te obezbijediti još jedan generator slučajnih brojeva za generisanje lažnih brojeva. Ključna prednost Bingo šeme u odnosu na ostale dostupne šeme za elektronsko glasanje jeste da ona omogućava glasaču da neposredno provjeri da je njegov glas ubrojan kandidatu za kog se opredijelio.

Bibliografija

[1] Election (political science), Encyclpoedia Britanica Online, Retrieved 18 August 2009

[2] Doc. dr Oliver Nikolić, Doc. dr Vladimir Đurić, Institut za uporedno pravo, Beograd, 2012 bibitemproces EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, December 7, 2007

[3] Prof. Dr. Jörn Müller-Quade, Improving and Analysing Bingo Voting, 5. Juli 2012

[4] Ammar Alkassar, Melanie Volkamer, E-Voting and Identity, Bochum, Germany, October 4-5, 2007

[5] Donald E Knuth, The Art of Computer Programming, Vol 2, 1998