HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost elektroničkog glasovanja

CCERT-PUBDOC-2007-04-188

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Izbori pojedinoj populaciji omogućuju odabir predstavnika u vlasti i izražavanje stajališta vezanih uz pitanja od općeg interesa. Integritet izbornog procesa jedan je od temelja demokracije i zbog toga on treba biti dovoljno robustan, kako bi se onemogućile različite zlonamjerne aktivnosti, ali i dovoljno transparentan, kako bi glasači i kandidati prihvatili rezultate glasovanja.

Sustav glasovanja, bio on elektronički ili klasičan sustav temeljen na papirnatim glasačkim listićima i različitim mehaničkim uređajima, treba zadovoljiti veći broj zahtjeva, od kojih su pojedini u određenoj mjeri oprečni. Prije svega potrebno je osigurati anonimnost glasača, kako bi ga se zaštitilo u slučaju glasanja protiv opresivne vlasti i kako bi se onemogućilo dokazivanje kojoj strani je otišao pojedini glas. U sustavima kod kojih glasač može dokazati za koga je glasovao postoji mogućnost kupovine pojedinih glasova od strane kandidata. Sustav glasovanja treba također biti otporan na različite oblike zlonamjernog djelovanja kao što su umetanje dodatnih glasačkih listića od strane glasača ili pogreške prilikom prebrojavanja glasova. Tijekom osmišljavanja sustava treba uzeti u obzir i tzv. ljudski faktor. Sustav glasovanja treba biti razumljiv i dostupan cjelokupnom glasačkom tijelu, bez obzira na dob i zdravstveno stanje. Ovakva široka dostupnost ozbiljan je logistički problem i na tom bi polju, uz pretpostavku zadovoljenja ostalih navedenih uvjeta, elektronički sustavi glasovanja trebali biti znatno bolji od klasičnih sustava.

U nastavku dokumenta ukratko su opisani oblici glasovanja, dana je analiza elektroničkih sustava glasovanja te su navedene moguće prijetnje takvim sustavima. Nakon toga slijede primjeri napada na elektroničke glasačke uređaje i sustave glasovanja putem Interneta te kratak opis nekolicine metoda njihove kontrole i nadzora.

2. Oblici glasovanja

Sustave glasovanja moguće je prema izvedbi podijeliti na:

- glasovanje papirnatim izbornim listićima,
- glasovanje perforiranim karticama,
- glasovanje pomoću optičkog čitača,
- glasovanje korištenjem mehaničkog glasačkog uređaja i
- elektroničko glasovanje

Pregled osnovnih karakteristika navedenih sustava glasovanja dan je tablicom *Tablica 1*.

KARAKTERISTIKA	TEHNOLOGIJA				
	papirnati listići	**perforirane kartice**	**optički čitač**	**mehanički uređaj**	**elektroničko glasovanje**
odabir kandidata	papir	papir	papir	označene mehaničke poluge	označeni izbori na računalnom zaslonu
lokalno prebrojavanje	ručno	elektroničko	elektroničko	ručno ili elektroničko	elektroničko
središnje prebrojavanje	elektroničko	elektroničko	elektroničko	elektroničko	elektroničko
mogućnost provjere izbora	da	da	da	ne	kod nekih sustava

Tablica 1: Pregled karakteristika sustava glasovanja

2.1. Glasovanje papirnatim izbornim listićima

Sustav glasovanja papirnatim izbornim listićima prvi je puta primijenjen u australskoj provinciji Viktoriji 1858. godine. Nakon utvrđivanja identiteta glasač dobiva glasački listić na kojemu označuje svoj izbor i kojega potom ubacuje u glasačku kutiju. Nakon zatvaranja birališta glasačke kutije se otvaraju, komisije prebrojavaju glasove i rezultate dojavljuju središnjici.

2.2. Glasovanje perforiranim karticama

Prilikom glasovanja perforiranim karticama (eng. *punchcard*) svaki glasač dobiva jednu karticu na kojoj posebno oblikovanim alatom uklanja perforaciju uz odabrani izbor. Nakon odabira kartice se ubacuju u glasačku kutiju ili u uređaj povezan s računalom. U upotrebi su dva tipa ovakvih kartica: *Votomatic* i *Datavote*. Kod *Votomatic* kartica je svaka perforacija označena brojem, dok su lista kandidata i upute za glasovanje dostupne na posebno tiskanim materijalima. Na *Datavote* karticama su uz perforacije otisnuta imena kandidata, odnosno opis mogućih izbora.

2.3. Glasovanje pomoću optičkog čitača

Kod glasačkih sustava koji koriste optičke čitače (eng. *scanner*) glasač dobiva glasački listić na kojemu označuje svoj izbor, npr. zacrnjivanjem polja uz odabranog kandidata. Listić se potom umeće u optički čitač koji bilježi glas. Pri tome je moguće upozoriti glasača ne neispravno ispunjen listić u slučaju odabira većeg broja kandidata od dozvoljenog ili u slučaju da na listiću nije odabran niti jedan kandidat.

2.4. Mehanički glasački uređaj

Glasovanje mehaničkim uređajem provodi se povlačenjem poluga od kojih je svaka pridružena jednom kandidatu. Izlaskom glasača iz kabine poluge se automatski vraćaju u početni položaj pri tome pokrećući sustav brojčanika. Ako je uređaj ispravan i ako su brojčanici prije otvaranja birališta postavljeni na nulu, stanje pojedinog brojčanika nakon zatvaranja birališta odgovara broju glasova

određenom kandidatu. Sustav mehaničkih ograničenja onemogućuje odabir većeg broja kandidata od dozvoljenog. Prvi mehanički glasački uređaji korišteni su krajem 19. stoljeća, a kako se danas više ne proizvode postupno ih se zamjenjuje elektroničkim uređajima.

2.5. Elektroničko glasovanje

Elektroničko glasovanje je širok pojam koji obuhvaća nekoliko različitih sustava glasovanja i prebrojavanja glasova. Elektronički uređaji koriste se u pojedinim fazama glasovanja kod sustava glasovanja perforiranim karticama i sustavima glasovanja pomoću optičkog čitača, a kod sustava koji za glasovanje koriste elektroničke kabine glasovanje se provodi u potpunosti elektronički. Ovim pojmom obuhvaćen je i prijenos pojedinih glasova ili rezultata glasovanja telefonom, privatnom računalnom mrežom ili Internetom.

Elektronički sustavi glasovanja pojavili su se 1960-ih godina s uvođenjem perforiranih kartica. Sustavi glasovanja pomoću optičkog čitača obuhvaćaju tzv. *marksense* čitače, EBM (*Electronic Ballot Marker*) uređaje, koji invalidima omogućuju glasovanje, i sustave s elektroničkom olovkom (eng. *digital pen*), koja ugrađenom kamerom bilježi glas označen na papirnatom glasačkom listiću radi lakšeg prebrojavanja. DRE (eng. *Direct-Recording Electronic*) glasački uređaji omogućuju preuzimanje i prikupljanje glasova, a koriste se kod svih izbora u Brazilu te u velikoj mjeri u Indiji, Nizozemskoj, Venezueli i Sjedinjenim Američkim Državama. Sustavi glasovanja putem Interneta koriste se u Estoniji i Švicarskoj.

Postoje i različiti hibridni sustavi kod kojih se glas daje elektroničkim putem (najčešće pomoću računalnog zaslona slično kao kod DRE sustava) nakon čega se ispisuje papirnati glasački listić s označenim izborom, koji glasaču omogućuje provjeru. Poseban uređaj koristi se potom za bilježenje glasa s pregledanog glasačkog listića.

2.5.1. DRE

DRE glasački sustavi omogućuju odabir kandidata putem elektroničko-optičkog uređaja, npr. računalnog zaslona osjetljivog na dodir (eng. *touchscreen*). Glasač prilikom dolaska na biralište i nakon provjere identiteta dobiva PIN (eng. *Personal Identification Number*) broj, elektroničku karticu (eng. *smartcard*) ili neku drugu oznaku (eng. *token*). Unošenjem spomenute oznake na glasačkom terminalu korisniku se omogućuje odabir među ponuđenim izborima. Nakon odabira kandidata glasaču se najčešće nudi uvid u učinjeni odabir i pruža mu se mogućnost izmjene ili ispravke nakon čega se glas smatra danim i korisnik može napustiti glasačko mjesto.

Potrebna obrada tako prikupljenih glasova provodi se programski unutar istog uređaja te se rezultati pohranjuju na prijenosnu memorijsku komponentu ili se ispisuju na papir nakon zatvaranja birališta. Postoje implementacije ovakvih sustava koje omogućuju prijenos pojedinih glasova ili rezultata glasovanja do centralnog mjesta za prikupljanje i obradu rezultata.

2.5.2. DRE sustavi koji koriste javnu mrežu

Pojedini DRE glasački sustavi za prijenos glasačkih podataka koriste javnu mrežu, npr. Internet ili telefonsku mrežu. Moguće je prenositi:

- pojedinačne glasove nakon njihova unošenja,
- periodički skupine glasova ili
- rezultate glasovanja nakon zatvaranja birališta.

Glasovanje preko Interneta moguće je implementirati na način da je glas moguće dati s bilo kojeg računala povezanog na Internet ili pomoću posebnih glasačkih uređaja povezanih na Internet, a koji su smješteni na glasačkim mjestima.

3. Analiza elektroničkog glasovanja

Sustavi elektroničkog glasovanja imaju brojne prednosti u odnosu na konvencionalne metode glasovanja. Elektronički uređaju mogu biti korišteni u različitim fazama glasačkog procesa, za:

- distribuiranje glasačkih listića i potrebne opreme,
- samo glasanje,
- prikupljanje glasova ili

- prebrojavanje glasova,

pa ovisno o tome mogu uvesti poboljšanja ili ranjivosti u pojedinu fazu.
Pojedini stručnjaci naglašuju kako ljudi ne mogu nadgledati procese unutar elektroničkog uređaja i kako zbog toga te operacije nisu vjerodostojne. Neki računalni stručnjaci proširuju ovu tvrdnju ističući kako pojedinac potpuno povjerenje može imati samo u programski kod kojega je sam autor.
U slučaju tajnog glasovanja nisu poznati korisnički unosi niti je moguće predvidjeti očekivane rezultate s kojima bi se usporedili ostvareni rezultati glasovanja pa rezultate glasovanja te preciznost, ispravnost i pouzdanost cjelokupnog elektroničkog sustava nije moguće provjeriti.
Zbog toga je potrebno da elektronički sustav tijekom glasovanja svakom korisniku na uvid da papirnati prikaz odabranog izbora. Takav papirnati prikaz uvjerava glasača da je njegov glas ispravno zabilježen, omogućuje otkrivanje kvara i prijevare te se može koristiti za provjeru elektronički prikupljenih glasova. Pored toga potrebno je omogućiti javni pristup i nadzor programske podrške elektroničkih uređaja koji sudjeluju u glasačkom procesu kako bi se osigurala njezina ispravnosti.

3.1. Glasačke oznake

Elektronički glasački sustavi mogu koristiti elektroničke glasačke oznake (eng. *ballot*). Time se uklanja mogućnost pomanjkanja glasačkih listića na pojedinom glasačkom mjestu kao i potreba za tiskanjem papirnatih glasačkih listića što može predstavljati značajan trošak.
U slučajevima kod kojih je to potrebno elektroničke glasačke oznake mogu biti programirane tako da omogućuju glasovanje na različitim jezicima na istom uređaju. Ako se tiskaju papirnati glasački listići na danim jezicima potrebno je odrediti koliko listića na kojem jeziku treba tiskati i koliko ih treba biti dostupno na pojedinom glasačkom mjestu. Dovoljan broj listića na svim jezicima i na svim glasačkim mjestima može se osigurati samo tiskanjem većeg broja listića, od kojih većina neće biti iskorištena.
Kritičari elektroničkih glasačkih oznaka ističu kako je potrebu za dodatnim glasačkim listićima na različitim jezicima moguće zadovoljiti tiskanjem istih na glasačkom mjestu. Uštedu na tiskanju papirnatih glasačkih listića osporavaju navodeći troškove provjere pojedinih koraka postavljanja elektroničkog sustava, koja može biti složena i skupa.

3.2. Dostupnost

Elektronički glasački uređaji mogu biti prilagođeni osobama s invaliditetom i tako ispuniti jedan od osnovnih zahtjeva na glasačke sustave, a to je zahtjev za dostupnošću sustava cjelokupnom glasačkom tijelu. Sustavi glasovanja perforiranim karticama i pomoću optičkih čitača nisu potpuno dostupni slijepim osobama i osobama s oštećenim vidom, dok sustavi glasovanja mehaničkim uređajima mogu predstavljati poteškoću osobama ograničene pokretljivosti i/ili snage. Elektronički uređaji mogu pomoću slušalica i drugih uređaja prilagođenih invalidnim osobama (eng. *adaptive technology*) ostvariti potrebnu razinu dostupnosti.

3.3. Kriptografska provjera

Sustavi elektroničkog glasovanja glasačima mogu omogućiti kriptografsku provjeru kako bi se uvjerili da je njihov glas ispravno unesen i pohranjen. Jedna od metoda kojima se takva provjera implementira je izdavanje elektroničke potvrde glasaču o danom glasu, a koja je digitalno potpisana od strane ovlaštenog glasačkog tijela. Na ovaj se način osigurava provjera ispravnosti danog glasa, ali i omogućuje zastrašivanje glasača i kupovina glasova jer opisani sustav ne osigurava anonimnost glasača.
Pojedini sustavi kriptografske provjere glasaču omogućuju provjeru danog glasa, ali mu onemogućuje dokazivanje izbora drugim osobama. Jedna od metoda ovakve provjere je izdavanje digitalno potpisane potvrde koja pored korisnikova sadrži i nasumično odabrane glasove drugih glasača. Korisnik na takvoj potvrdi može pronaći svoj glas i utvrditi je li ispravno unesen, ali ne može pomoću iste dokazati kakav je bio njegov glas. Također je moguće svakom glasu pridijeliti nasumično stvoreni identifikacijski broj glasačke sjednice koji glasaču omogućuje provjeru svoga glasa tijekom javne revizije glasovanja.

3.4. Glasačeva namjera

Elektronički uređaji mogu glasaču dati trenutnu povratnu informaciju upozoravajući ga u slučaju neispravnog glasa. Glas može biti neispravan ako je odabran veći broj kandidata od dozvoljenog (eng. *over-vote*) ili ako nije odabran niti jedan kandidat (eng. *under-vote*). Na ovaj način uređaj može utvrditi koja je glasačeva namjera, odnosno radi li se o nenamjernoj pogrešci ili glasač želi potrošiti svoj glas bez da ga da ijednom kandidatu.

3.5. Kontrola

Osnovna poteškoća kod svih, ne samo elektroničkih, glasačkih uređaja je osiguravanje ispravnog bilježenja i pohranjivanja glasova. Ovo je posebno teško osigurati i provjeriti kod sustava bez papirnatih glasačkih listića. Zbog toga se takvim glasačkim sustavima dodaju neovisni nadzorni uređaji koji omogućuju ponovno prebrojavanje glasova i razne oblike nadzora nad glasačkim sustavom.

Nadzorni sustavi glasačima mogu omogućiti:

- provjeru ispravnosti bilježenje njihova glasa,
- provjeru njegove pohrane,
- otkrivanje pokušaja prijevare,
- otkrivanje kvara glasačkog uređaja te
- nadzor nad njim.

Tehnologije koje se pri tom koriste su:

- kriptografija – vizualna ili matematička,
- papirnati dokument – glasač ga zadržava ili samo provjerava,
- zvučna provjera i
- dvostruko bilježenje.

3.6. Sigurnosni kriteriji

Sigurnosni kriteriji koje bi elektronički glasački sustavi trebali zadovoljiti definirani su unutar pojedinih država u kojima se takvi sustavi koriste, npr. u Sjedinjenim Američkim Državama ovi kriteriji propisani su U.S. TCSEC (eng. *United States Trusted Computer System Evaluation Criteria*), u Europskoj Uniji ITSEC (eng. *Information Technology Security Evaluation Criteria*), a u Kanadi CTCPEC (eng. *Canadian Trusted Computer Product Evaluation Criteria*) dokumentom.

Općeniti sigurnosni kriteriji su:

- **Nepovredivost sustava** – računalni sustav, sklopovlje i programsku podršku, potrebno je zaštititi od neovlaštenih izmjena (eng. *tamperproof*). Potrebno je onemogućiti promjene u sustavu tijekom svih aktivnih faza glasovanja. To se odnosi na programski kod, početne parametre i sve postavke koje nakon dobivanja certifikata više nije dozvoljeni mijenjati. Također nije dozvoljeno korištenje programskog koda koji se mijenja tijekom izvođenja (eng. *run-time self-modifying*). Postupak pokretanja sustava (eng. *bootload*) potrebno je zaštititi od napada koji mogu rezultirati umetanje zlonamjernih aplikacija kakve su tzv. trojanski konji.
- **Pouzdanost i nepovredivost podataka** – sve podatke vezane uz unošenje i pohranjivanje glasova potrebno je zaštititi od neovlaštenog pristupa i izmjena.
- **Anonimnost glasača i povjerljivost podataka** – pristup broju glasova potrebno je tijekom glasovanja u potpunosti onemogućiti. Unutar sustava ne smije postojati poveznica između pohranjenih glasova i identiteta glasača.
- **Autorizacija operatera** – osobama zaduženima za vođenje izbornog mjesta pristup elektroničkom glasačkom sustavu potrebno je omogućiti uz netrivijalne metode autorizacije. Statičke korisničke zaporke općenito nisu prikladne. Alternativni načini pristupa sustavu (eng. *trapdoor*), uobičajeno korišteni tijekom postavljanja i održavanja, nisu dozvoljeni kod glasačkih sustava.
- **Nadzor** – sve postupke unutar sustava potrebno je neprestano nadzirati, uz ograničenja nužna kako bi se očuvala anonimnost glasača. Nadzor mora obuhvaćati zabilježene i pohranjene glasove te sve programske i administrativne intervencije unutar sustava, kao što

su npr. testiranja prije i poslije izbora. Sve pokušaje izmjena sustava, naročito one koji se kose sa zahtjevom na nepovredivost sustava, potrebno je zabilježiti. Također je potrebno bilježiti prijave i ostale radnje operatera. Sustav nadzora mora biti građen tako da ga je nemoguće isključiti ili zaobići.

- **Ispitivanje** – sklopovlje, asemblerski programski kod (eng. *microcode*), programska podrška i dokumentacija elektroničkog sustava za glasovanje treba u svakom trenutku biti dostupna za ispitivanje bez obzira na moguća upozorenja proizvođača kako bi se time mogla ugroziti sigurnost sustava.
- **Dostupnost** – potrebno je sustav zaštititi od slučajnog i zlonamjernog uskraćivanja usluga kako bi bio bez prekida dostupan za vrijeme glasovanja.
- **Pouzdanost** – tijekom razvoja sustava, njegove implementacije i održavanja potrebno je minimizirati mogućnost pojavljivanja slučajnih pogrešaka i umetanja zlonamjerno oblikovanog programskog koda.
- **Sučelje** – sustava potrebno je oblikovati tako da omogućuje njegovo jednostavno korištenje od strane lokalnih službenika angažiranih u vođenju pojedinog glasačkog mjesta, bez potrebe za sudjelovanjem udaljenog osoblja putem Interneta. Ono treba biti otporno na kvarove (eng. *fail-safe*) i na pogreške tijekom korištenja (eng. *fool-proof*) te treba sadržavati opširne mehanizme sprječavanja slučajne ili namjerne zloupotrebe.
- **Dokumentacija** – razvoj, implementacija, načini korištenja te metode testiranja elektroničkog glasačkog sustava potrebno je opširno i dosljedno dokumentirani. U takvoj dokumentaciji potrebno je navesti i jamstva ispravnosti svih aspekata sustava.

4. Moguće prijetnje elektroničkom glasovanju

Pet osnovnih prijetnji elektroničkom glasovanju su:

1. onemogućavanje glasovanja,
2. neovlaštena izmjena glasa,
3. ugrožavanje anonimnosti glasača,
4. višestruko glasovanje i
5. trgovanje glasovima.

Računalni sustavi omogućuju automatiziranje i ubrzavanje izvođenja jednostavnih zadataka što s druge strane može olakšati izvođenje napada i otežati posljedice u slučaju njegovog uspješnog provođenja. Navedene prijetnje izraženije su u slučaju napada većih razmjera, naročito kod centraliziranih sustava kod kojih jedna iskorištena ranjivost može utjecati na stotine tisuća glasača.

4.1. Onemogućavanje glasovanja

Na rezultate izbora moguće je utjecati onemogućavanjem glasovanja pojedinim glasačima ili skupinama glasača ovisno o procjeni vjerojatnosti kakav bi njihov glas mogao biti. Glasovanje putem Interneta naročito je pogodno za ovakve napade. Praćenjem korisnikovih internet aktivnosti moguće je procijeniti kakav će njegov glas biti i na temelju toga mu omogućiti, odnosno onemogućiti, glasovanje. Takve napade je izrazito teško otkriti, a još teže ukloniti njihove posljedice.

4.2. Izmjena glasa

Izmjena glasa kod konvencionalnih sustava s papirnatim glasačkim listićima provodi se jednostavnim dodavanjem oznake uz kandidata kojega glasač nije odabrao ili obezvrjeđivanjem listića odabirom većeg broja kandidata od dopuštenog. Elektronički sustavi pružaju nove i raznolike mogućnosti izmjene glasova. Zlonamjernim izmjenama sklopovlja i/ili programske podrške elektroničkog glasačkog uređaja moguće je provoditi selektivnu krađu glasova u korist jednog ili više kandidata, ovisno o tijeku glasovanja. Kod glasovanja putem Interneta presretanjem komunikacije između glasačeva računala i poslužitelja moguće je izmijeniti glas napadnutog korisnika.

4.3. Ugrožavanje anonimnosti glasača

Kako bi se glasače zaštitilo od iznuđivanja i kako bi se spriječila trgovina glasovima potrebno je onemogućiti povezivanje pojedinog glasača s njegovim glasom. Kod glasovanja papirnatim glasačkim listićima to je ostvareno pojedinačnim označavanjem listića u zaklonjenim glasačkim mjestima i miješanjem listića unutar glasačke kutije. Elektronički glasački sustavi pružaju brojne mogućnosti ugrožavanja anonimnosti glasača.

4.4. Višestruko glasovanje

Sustavi glasovanja putem Interneta naročito su osjetljivi na napade višestrukim glasovanjem. Praćenjem navika registriranih glasača moguće je utvrditi koji od njih najvjerojatnije neće glasati te potom automatiziranim napadom krađe njihova identiteta ostvariti veći broj lažnih glasova.

4.5. Trgovanje glasovima

Trgovanje glasovima usko je vezano uz problem osiguravanja anonimnosti glasača. Ako pojedini glasač može dokazati kojem kandidatu je dao glas postoji mogućnost da ga nepošteni kandidat za to novčano nagradi. Elektronički sustavi, prije svega sustavi glasovanja putem Interneta, mogu u slučaju ranjivosti omogućiti trgovinu glasovima većih razmjera.

5. Napadi na elektroničke glasačke uređaje

5.1. Izmjena programske podrške

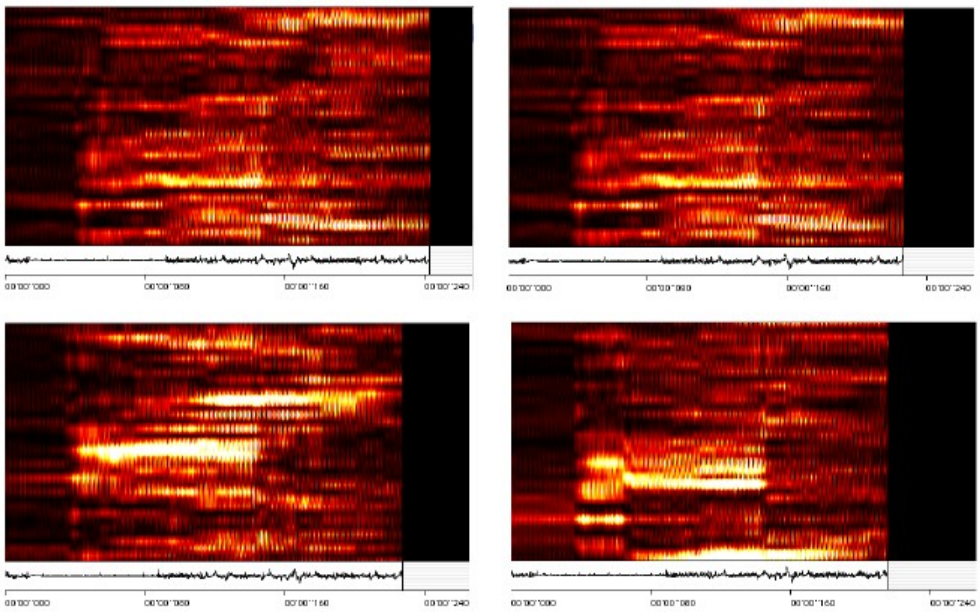
Ovaj napad provodi se izmjenom programske podrške elektroničkog glasačkog uređaja ili umetanjem novog, zlonamjerno oblikovanog, programskog koda. Umetanje novog programskog koda moguće je izvesti njegovim pohranjivanjem unutar postojećih memorijskih elemenata uređaja ili umetanjem novog sklopovlja s zlonamjernim kodom, npr. EPROM (eng. *Erasable Programmable Read-Only Memory*) čipova.

Zlonamjerno oblikovani programski kod moguće je oblikovati tako da analizom unesenih podataka određuje radi li se o ispitivanju uređaja ili stvarnim izborima i na temelju toga samostalno odluči o izmjeni rezultata ili prikrivanju svoga postojanja. Također ga je moguće podesiti da pretražuje imena na listama kandidata i u skladu s rezultatima pretrage utječe na raspodjelu glasova. Ovime se omogućuje umetanje zlonamjernog programskog koda prije objave lista kandidata i varanje na izborima kroz dulji niz godina.

5.2. Napad analizom zračenja

Mnogi elektronički uređaji, kojima to nije namjena, emitiraju zračenje u području radio signala. U slučaju računalnih sustava takva zračenja mogu otkriti aktivnosti koje se izvode na prisluškivanom računalu. Za prisluškivanje uređaja potrebno je snimiti zračenje pomoću odgovarajuće antene i prijemnika nakon čega se provodi analiza snimljenog signala pomoću spektralnog analizatora.

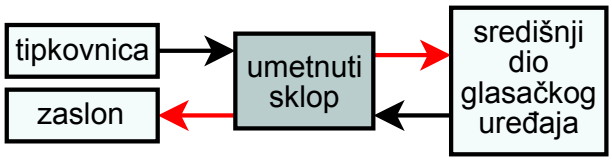
Snimanjem emisije radio signala elektroničkog uređaja za glasovanje moguće je u određenim situacijama utvrditi način glasovanja pojedinog birača. Na slici *Slika 1* prikazana su četiri signala snimljena tijekom ispisivanja imena kandidata na ekranu *Nedap/Groenendaal ES3B* elektroničkom uređaju za glasovanje pomoću kojega 90% nizozemskih glasača sudjeluje u glasovanju. Dvije snimke u gornjem redu snimljene su u slučaju odabira istog kandidata, dok su na druge dvije snimke prikazani signali snimljeni tijekom prikaza imena drugih kandidata. Očito je kako se na temelju snimljenih uzoraka može odrediti za koga je pojedini glasač glasovao.



Slika 1: Signali snimljeni tijekom prikaza imena kandidata na ekranu Nedap/Groenendaal ES3B uređaja

5.3. Simuliranje sučelja

Umetanjem posebno oblikovanog sklopa između sučelja i središnjeg dijela elektroničkog glasačkog uređaja moguće je izvesti tzv. MITM (eng. *Man In The Middle*) napad. Takav sklop presreće podatke unesene putem tipkovnice, po potrebi ih izmjenjuje i prosljeđuje središnjem dijelu uređaja. Sličan postupak provodi se i u suprotnom smjeru: signali namijenjeni zaslonu se presreću, izmjenjuju i tek nakon toga prikazuju. Na slici *Slika 2* vjerodostojni signali prikazani su strelicama crne boje, dok su krivotvoreni signali prikazani crvenim strelicama.



Slika 2: Umetnuti sklop simulira sučelje glasačkog uređaja

Umetnuti sklop moguće je programirati tako da tijekom unošenja prvog glasa nakon otvaranja birališta snimi podatke vezane uz liste kandidata. Također ga je moguće postaviti tako da se pokuša prikriti uočavanjem razlike između ispitivanja uređaja i stvarnih izbora.

Ovaj napad moguće je prilagoditi i uređajima koji umjesto tipkovnice imaju zaslone osjetljive na dodir. Zlonamjerno oblikovani sklop se umeće izvan središnjeg dijela glasačkog uređaja pa je, ovisno o njegovoj fizičkoj građi, sklop moguće umetnuti bez oštećivanja eventualnih pečata koji štite glavno kućište.

5.4. Socijalni inženjering

Socijalni inženjering pripada skupini napada na računalne sustave, ali i sustave u širem smislu riječi, a svodi se na nagovaranja ljudi da ispune zahtjeve napadača. Radi se o načinu stjecanja informacija i podataka do kojih napadač legitimnim putem ne bi mogao doći. Pri tome se ne iskorištavaju propusti implementacija operacijskih sustava, protokola i aplikacija, nego se napad usmjerava na korisnika.

U ovu skupinu spadaju napadi kod kojih zlonamjerni korisnik hini kako starijoj ili slijepoj osobi želi pomoći u glasovanju i pri tome unosi glas prema svom nahođenju. Drugi napad iz ove skupine provodi zlonamjerni službenik koji vodi glasačko mjesto, a sastoji se od davanja neispravnih uputa o načinu glasovanja. Glasovi krivo upućenih glasača ne bivaju uneseni pa napadač može glasovati umjesto njih.

5.5. Napadi na identifikacijske oznake

Kod elektroničkih sustava za glasovanje koji koriste elektroničke identifikacijske oznake, npr. kartice (eng. *smatrcard*), moguće je u slučaju nesigurne implementacije krivotvoriti ove oznake i pomoću njih višestruko glasovati ili ostvariti neovlašten pristup glasačkom uređaju.
Dobar primjer za ilustraciju ovakvog napada je *Diebold AccuVote-TS* glasački uređaj (*Slika 3*) korišten u Sjedinjenim Američkim Državama. Ovaj sustav ne iskorištava glavnu prednost elektroničkih kartica; mogućnost implementiranja kriptografskih algoritama unutar njih samih. Tim propustom su krivotvorenje kartica, a samim time i napad na sustav, uvelike olakšani.

Slika 3: *Diebold AccuVote-TS* glasački uređaj (s čitačem kartica u donjem desnom uglu)

5.6. Krivotvorenje rezultata

Elektronički glasački sustav može biti oblikovan tako da pojedini uređaj prikupljene glasova dostavlja pozadinskom poslužitelju koji ih pohranjuje. Napadač može prisluškivanjem veze uređaja sa spomenutim poslužiteljem prikupiti dovoljno podataka potrebnih za krivotvorenje takvih poruka. U slučaju uspješnog izvođenja napada poslužitelj napadača prihvaća kao jednog ili više glasačkih uređaja, preuzima lažne izvještaje o glasovanju i pohranjuje ih.

6. Napadi na sustave glasovanja putem Interneta

Napadi na sustave glasovanja putem Interneta mogu se podijeliti u tri skupine:

- napadi pomoću zlonamjernih aplikacija na korisničkom računalu,
- napad na vezu korisničkog računala s glasačkim poslužiteljem i
- socijalni inženjering.

6.1. Zlonamjerne aplikacije

Zlonamjerno oblikovana aplikacija prisutna na glasačevom računalu može neprimjetno izmijeniti njegov glas, bez obzira na primijenjene metode autorizacije i enkripcije. To je moguće jer se napad izvodi prije provođenja autorizacije korisnika i prije enkripcije podataka. Nakon uspješne izmjene glasa zlonamjerna se aplikacija može automatski izbrisati uklanjajući tako podatke koji bi mogli omogućiti otkrivanje napada i ispravak učinjene štete.
Primjeri ovakvih aplikacija su *Backorifice 2000* (BO2K) paket i *Chernobyl* (CIH) računalni virus. BO2K je programski paket otvorenog programskog koda namijenjen upravljanju radom računalne mreže. Građen je tako da je izrazito teško otkriti njegovo prisustvo na računalu, a posjeduje mogućnost udaljenog upravljanja računalom na kojem je instaliran. Činjenica da se radi o paketu otvorenog programskog koda napadaču omogućuje unošenje zlonamjernih izmjena koje mu mogu omogućiti preuzimanje potpune kontrole nad napadnutim računalom. U slučaju uspješnog izvođenja napada zlonamjerni korisnik može nadgledati glasovanje i izmijeniti korisnikov glas.
CIH virus aktivirao se 26. travnja 1999. godine te izmjenama BIOS (eng. *Basic Input/Output System*) ugrađene programske podrške brojnih računala onemogućio njihovo pokretanje. Sličan virus mogao bi aktiviranjem neposredno prije početka izbora onemogućiti glasovanje velikom broju korisnika. Napad je moguće oblikovati tako da se virus proširi samo na ciljane demografske skupine.

6.2. Napadi na vezu s poslužiteljem

Kod sigurno oblikovanog sustava glasovanja putem Interneta podaci se između klijentskog računala i glasačkog poslužitelja razmjenjuju zaštićeni nekom od prihvaćenih kriptografskih metoda. Zbog toga je ova veza prije svega osjetljiva na napade uskraćivanjem usluga. Distribuirana inačica ovog napada (eng. *Distributed Denial of Service – DDOS*) provodi se automatskim instaliranjem velikog broja pozadinskih aplikacija (eng. *daemon*) na različitim računalima. Glavna aplikacija (eng. *master*) u trenutku napada spomenutim pozadinskim aplikacijama dojavljuje podatke o meti kojoj one potom šalju velik broj poruka. Napadnuti sustav zauzet je obradom ogromnog broja poruka što rezultira uskraćivanjem usluga. Ovakav napad na glasački poslužitelj na dan izbora u potpunosti bi onemogućio glasovanje.

Mogući su i drugačije oblikovani napadi kojima se glasanje može onemogućiti pojedinim korisnicima ili skupinama korisnika. Primjer takvog napada je tzv. *ping of death* napad koji se provodi slanjem posebno oblikovane poruke razlomljene na dva ili više podatkovnih paketa. Nakon primitka ovih paketa napadnuto računalo rekonstruira izvornu poruku koja je tako oblikovana da uzrokuje njegovo rušenje.

6.3. Socijalni inženjering

Socijalni inženjering u slučaju glasovanja putem Interneta svodi se na podmetanje posebno oblikovane web stranice umjesto one na kojoj se provodi glasovanje. Korisnik uvjeren da unosi svoj glas na takvoj stranici zapravo napadaču predaje svoje autorizacijske podatke i omogućuje mu krađu glasa.

Lažnu web stranicu za glasovanje moguće je podmetnuti na više načina:

- slanjem elektroničkog pisma u kojemu se nalazi poveznica (eng. *link*) na nju,
- otimanjem korisničke sjednice preusmjeravanjem prometa ili
- tzv. *cache poisoning* ili nekim drugim napadom na DNS (eng. *Domain Name Service*) uslugu.

Postoje brojne metode provjere vjerodostojnosti web stranice, ali je iluzorno očekivati kako će ih prilikom glasovanja primijeniti značajniji broj glasača.

Osim krađe glasova moguće je provesti napad usmjeravanjem veze na računalo koje glumi glasački poslužitelj, ali samo prikuplja glasove bez njihova prosljeđivanja. Preusmjeravanjem glasova iz Internet kafića ili knjižnice u područjima za koja je poznato da glasaju na određeni način moguće je utjecati na rezultate izbora.

7. Kontrola i nadzor

7.1. VVPAT

VVPAT (eng. *Voter Verified Paper Audit Trail*) je neovisan sustav provjere glasačkih uređaja koji je osmišljen s ciljem uvjeravanja glasača u ispravnost preuzimanja i pohrane glasova, otkrivanja prijevara i kvarova te omogućavanja nadzora cjelokupnog elektroničkog glasačkog sustava.

Ovaj se sustav temelji na dvije osnovne razlike između papira i računala kao medija pohranjivanja glasova. Prva razlika je u tome što je papir moguće izravno čitati dok je za čitanje računalne memorije potrebno vjerodostojno sklopovlje i programska podrška. Papirnati dokument je uz to znatno teže izmijeniti od podataka pohranjenih u računalnoj memoriji.

7.2. E2E nadzor

E2E (eng. *End-to-end*) su sustavi neovisnog nadzora koji pohranjuju kriptirane kopije glasova. Pojedine implementacije omogućuju izdavanje pisanih potvrda kojima se:

- glasaču potvrđuje kako je njegov glas preuzet i pohranjen,
- osigurava da su sve glasove dali vjerodostojni glasači i
- omogućuje naknadna provjera rezultata glasovanja.

Ovaj sustav može koristiti elektroničku ili vizualnu kriptografiju. Elektronička kriptografija koristi se npr. kod *VoteHere* sustava za glasovanje dok kod sustava koji koriste vizualnu kriptografiju, nakon odabira kandidata, DRE uređaj ispisuje posebno oblikovani glasački listić na dva prozirna lista. Kada se

ova dva sloja stave jedan iznad drugoga tvore čitljivu potvrdu o glasu. Pojedini sloj je kriptiran nekim oblikom vizualne kriptografije i sam za sebe ne omogućuje otkrivanje podataka o glasu. Glasač odabire jedan od slojeva kojega uništava na licu mjesta dok drugi sloj zadržava kao osiguranje da njegov glas neće biti naknadno izmijenjen. Glasački uređaj pohranjuje elektroničku inačicu uništenog sloja.

7.3. Paralelno ispitivanje

Paralelno ispitivanje elektroničkih glasačkih uređaja provodi se unosom podataka koji se ne razlikuju od onih koji bi bili unošeni u slučaju stvarnih izbora. Uređaj se tijekom ovakvog ispitivanja tretira kao tzv. crna kutija, promatraju se samo podaci uneseni u njega i rezultati koje uređaj daje na izlazu. Uređaji za ispitivanje nasumično se odabiru na dan izbora prije otvaranja birališta, zamjenjuju se pričuvnim uređajima i odvoze na ispitivanje. Tijekom izbora na tim se uređajima simulira glasovanje uz pomno bilježenje unesenih glasova te se, po zatvaranju birališta, uspoređuju rezultati glasovanja koje daju ispitivani uređaji s očekivanim rezultatima.

Kako bi se zadovoljila postavljena razina sigurnosti elektroničkog glasačkog sustava potrebno je paralelnom ispitivanju podvrći određen udio uređaja. Također je potrebno uspostaviti prave mehanizme koji će, u slučaju otkrivenih nepravilnosti, omogućiti ponovno održavanje izbora ili odgađanje prihvaćanja rezultata izbora dok se ne provede potpuna istraga.

Kako bi se potencijalnoj umetnutoj zlonamjernoj aplikaciji onemogućilo razlikovanje ispitivanja od stvarnih izbora, a time i njezino prikrivanje, ispitivanje treba što više nalikovati stvarnim izborima. To znači da trajanje ispitivanja i broj glasova unesenih tijekom istoga trebaju odgovarati vrijednostima kod pravog glasanja. Kako bi se onemogućilo otkrivanje ispitivanja na temelju statističke analize vremena između unošenja glasova poželjno je da ga provodi robot ili da se ljudski ispitivači učestalo izmjenjuju. Jedan ispitivač bi naime nakon nekog vremena vjerojatno počeo glasove unositi određenim ritmom.

Paralelno ispitivanje nije univerzalno rješenje i ne može otkriti sve prijevare. Na primjer, moguće je glasački uređaj podesiti tako da očekuje određeni niz pritisaka tipki, tzv. *magic button*, nakon kojega slijedi unošenje glasa. Ako navedeni niz radnji aktivira krađu glasova paralelnim ispitivanjem ga nije moguće otkriti.

7.4. Ispitivanje sklopovlja i programske podrške

Prije i/ili nakon izbora moguće je ispitati sklopovlje elektroničkog glasačkog uređaja i programske podrške pohranjene u njemu. Jednostavnim vizualnim pregledom moguće je, nakon otvaranja kućišta, utvrditi jesu li u uređaj naknadno ugrađene dodatne sklopovske komponente. Ispitivanje programske podrške provodi se njenim učitavanjem iz memorijskih elemenata uređaja i usporedbom s izvornom programskom podrškom. Osim izravnim uspoređivanjem programskog koda moguće je provjeru provesti uspoređivanjem kontrolnih suma koda, takozvanih *hash* vrijednosti.

8. Zaključak

Elektronički sustavi glasovanja imaju brojne prednosti pred konvencionalnim glasačkim sustavima. Zamjena papirnatih glasačkih listića elektroničkim sustavima omogućuje značajne uštede te pruža mogućnosti jednostavne prilagodbe sustava glasačima koji se koriste različitim jezicima i osobama narušena zdravlja. Različite metode kriptografskih provjera omogućuju provjeru rada sustava za glasovanje, a ako dođe do neispravnog glasovanja glasač je na to odmah upozoren.

Usporedno s brojnim naprednim mogućnostima pojavljuju se i ranjivosti ovakvih sustava. Nesigurno implementirani sustav zlonamjernom korisniku može omogućiti sprječavanje pojedinih glasača ili skupina glasača da sudjeluju u glasovanju, krađu glasova njihovom izmjenom, otkrivanje identiteta glasača ili višestruko glasovanje. Mogućnost automatizacije zadataka pomoću računalnih sustava olakšava ovakve napade i u slučaju uspješnog izvođenja napada može rezultirati posljedicama širokih razmjera.

Zbog svega navedenog potrebno je prijelaz s konvencionalnih na elektroničke sustave glasovanja provesti pažljivo i postupno uz opširnu javnu raspravu i nadzor. Nadzor sustava potrebno je provoditi prije, tijekom i nakon glasovanja uz opširno dokumentiranje svih koraka postavljanja i ispitivanja. Kako bi se omogućila provjera unosa glasa, otkrivanje prijevara i kvarova te eventualno naknadno prebrojavanje glasova elektronički sustav za glasovanje treba proizvesti papirnati trag kojim se ne ugrožava anonimnost glasača.

9. Reference

[1] Todayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach: Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy 2004, 2004.

[2] Overview of Voting Technologies, http://www.verifiedvotingfoundation.org/article.php?id=5135, ožujak 2007.

[3] Vote, http://americanhistory.si.edu/vote/, ožujak 2007.

[4] Douglas W. Jones: Voting and Elections, http://www.cs.uiowa.edu/~jones/voting/, ožujak 2007.

[5] Punchcards, http://www.fec.gov/pages/punchrd.htm, ožujak 2007.

[6] Electronic voting, http://en.wikipedia.org/wiki/Electronic_voting, ožujak 2007.

[7] Peter G. Neumann: Security Criteria for Electronic Voting, http://www.csl.sri.com/users/neumann/ncs93.html, ožujak 2007.

[8] David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner: A Security Analysis of the Secure Electronic Registration and Voting Experiment, http://www.servesecurityreport.org/paper.pdf, ožujak 2007.

[9] Rop Gonggrijp, Willem-Jan Hengeveld: Nedap/Groenendaal ES3B voting computer, http://www.wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf, ožujak 2007.

[10] Avi Rubin: Security Considerations for Remote Electronic Voting over the Internet, http://avirubin.com/e-voting.security.html, ožujak 2007.

[11] Electoral fraud, http://en.wikipedia.org/wiki/Electoral_fraud, ožujak 2007.

[12] Voter Verified Paper Audit Trail, http://en.wikipedia.org/wiki/VVPAT, ožujak 2007.