

Elektronske volitve

(CC) 2022

Matej Kovačič

<https://telefoncek.si>



This work is published under
CC BY-NC-SA 4.0 license

Elektronske volitve

“Elektronske” volitve:

- elektronsko štetje klasičnih glasovnic;
- oddaja elektronske glasovnice.

Elektronsko glasovnico je mogoče oddati:

- na volišču, s pomočjo posebne naprave (svojem matičnem ali kateremkoli);
- na daljavo (npr. preko interneta).

Različne prednosti: od hitrosti pridobitve rezultatov do udobnosti za volivca.

Za volivce je verjetno enostavnejša izvedba elektronskih volitev, kot internetnih volitev: bankomati vs. internet.

Prednosti elektronskih volitev

Odvisne od načina glasovanja:

- možnost prehodov med volišči;
- omogoča oddajo glasu prizadetim osebam;
- hitrejša ugotovitev rezultatov;
- manjša možnost napak (neveljavne glasovnice?);
- zvišanje volilne udeležbe;
- možnost uporabe multimedijskih elementov npr. prikaz slikovnega gradiva, zvočna navodila za glasovanje...);
- posredno: več neposredne demokracije.

Slabosti elektronskih volitev

Tajnost volitev (anonimnost in "volilni obred", možnosti preprodaje glasov);

Transparentnost volitev (upravljanje z informacijskim sistemom zahteva strokovnjake);

Višja cena (odvisno od pogostosti volitev), strojna oprema med volitvami zastari;

Zanesljivost volitev in možnost okvar (kaj če informacijski sistem preneha delovati);

Veljavnost rezultatov - možnosti napak ali ponarejanja izida volitev;

Nezmožnost oddaje neveljavne glasovnice (?);

Digitalna ločnica ter seznanjenost (znanje) volivcev z elektronsko tehnologijo;

Zahteve elektronskih volitev

- Splošne.
- Svobodne (brez oglasov, zavestno nepravilno glasovanje).
- Enakopravne (en volivec – en glas).
- Tajne (uravnoveženost tajnosti in transparentnosti; naj ne omogoča preprodaje glasov (npr. z možnostjo izpisa potrdila, ki potrjuje kako je volivec glasoval)).
- Neposredne (brez posrednikov).

Zahteve elektronskih volitev

	ZAKONSKE ZAhteVE	SPLOŠNE SISTEMSKe ZAhteVE
1	Splošne	Uradno enakovreden klasičnim volitvam
		Izvoljivost – registracija in identifikacija
2	Svobodne	Odsotnost vplivanja na volivce
		Brez reklamnih volilnih oglasov na portalu e-volitev
		Možnost zavestnega nepravilnega glasovanja
3	Enakopravne	Enakopravnost kandidatov
		Enakopravnost volivcev
		En volivec – en glas
4	Tajne	Tajnost
		Uravnoteženost tajnosti in transparentnosti
5	Neposredne	Avtonomno beleženje in preštevanje glasovnic
6	Demokratične	Zaupanje in transparentnost
		Preverljivost in nadzorljivost
		Zanesljivost in varnost
		Enostavnost

Vir: Študija izvedljivosti e-volitev s predlogi implementacije, 2004 (avtorja Turk in Györkös).

Nekatere grožnje e-volitvam

Odvzem volilne pravice (DOS napad na informacijski sistem).

Spreminjanje izpolnjene glasovnice.

Izguba zasebnosti.

Večkratno glasovanje.

Preprodaja glasov.

Volilne naprave

Elementi:

- zaslon občutljiv na dotik;
- pomnilnik za zanesljivo shranjevanje glasovnic;
- možnost alternativnega izpisa volivčeve volje (tim. "*paper trail*");
- identifikacija volivca;
- varnost;
- enostavnost uporabe za volivca ter člane volilne komisije.

Volilne naprave



Volilna naprava v Braziliji, foto (CC): Antonio Cruz/ABr



Volilna naprava v Avstraliji, foto (C): Phillip Green - ACT Electoral Commission, <<http://www.recul-democratique.org/eVACS.html>>

Volilne naprave

Electorate of Ginninderra

Select five candidates in the order of your choice. You may then select as many further candidates as you wish.

A AUSTRALIAN DEMOCRATS <input checked="" type="checkbox"/> Roslyn DUNDAS <input checked="" type="checkbox"/> Dan McMILLAN <input type="checkbox"/> Anthony DAVID	B THE ACT GREENS <input type="checkbox"/> Shane RATTENBURY <input type="checkbox"/> Patricia WOODCROFT-LEE	C GUNGAHLIN EQUALITY PARTY <input type="checkbox"/> John SIMMONS <input type="checkbox"/> Gail JONES
D DAVE RUGENDYKE <input type="checkbox"/> Ian BROWN <input type="checkbox"/> Dave RUGENDYKE	E LIBERAL DEMOCRATIC PARTY <input type="checkbox"/> Susan MORRISSEY <input checked="" type="checkbox"/> John HUMPHREYS	F <input checked="" type="checkbox"/> Geoff CLARKE <input type="checkbox"/> Darcy HENRY
G LIBERAL PARTY <input type="checkbox"/> Vicki DUNNE <input type="checkbox"/> Ilona FRASER <input type="checkbox"/> Harold HIRD <input type="checkbox"/> Bill STEFANIAK <input type="checkbox"/> Andrew SARRI	H AUSTRALIAN LABOR PARTY <input type="checkbox"/> Wayne BERRY <input type="checkbox"/> Vic REBIKOFF <input type="checkbox"/> Susan McCARTHY <input type="checkbox"/> Judith DOWNEY <input type="checkbox"/> Jon STANHOPE	UNGROUPED <input type="checkbox"/> Rhonda JAMES NURSES GOOD GOVERNMENT PARTY <input type="checkbox"/> Chris GARVIE INDEPENDENT <input type="checkbox"/> Shaun GOOD INDEPENDENT

Volilna naprava v Avstraliji, foto (C): Phillip Green - ACT Electoral Commission, <<http://www.recul-democratique.org/eVACS.html>>

Začetki . . .

ZDA, leta 2000: številni problemi z okvarami naprav, posledica katerih je bilo onemogočeno glasovanje ter sporočaje rezultatov, napačno preštevanje glasov, sumi volilnih goljufij, leta 2003 se razkrijejo številne nepravilnosti pri proizvajalcu volilnih naprav Diebold, očitki o privatizaciji volitev, nameščanje neavtoriziranih posodobitev....

Avstralija: leta 2001, odprtokodne, sistem EVACS temeljil na Linuxu.

Estonija: prve volitve preko interneta leta 2005, parlamentarne volitve leta 2007.

Švica 2004, najprej preko interneta, s SMS sporočili in preko ITV (*interactive television systems*), leta 2007 so SMS glasovanje opustili.

Na Nizozemskem so oktobra 2007 prepovedali uporabo elektronskih volilnih naprav zaradi možnosti ponarejanja, v Nemčiji pa leta 2009.

Splošno o varnosti

Gre za varovanje elektronskih glasovnic pred nepooblaščenim dostopom, uporabo, razkritjem, uničenjem, spreminjanjem ali izgubo.

Gre tudi za varovanje zasebnosti volivca in zagotavljanje tajnosti glasovanja.

Glasovalne naprave – ali glasovalni računalniki?

Kraja klasičnih volitev zahteva široko zaroto, kaj pa kraja elektronskih volitev?

“*Single point of failure*” pri sistemu internetnih volitev?

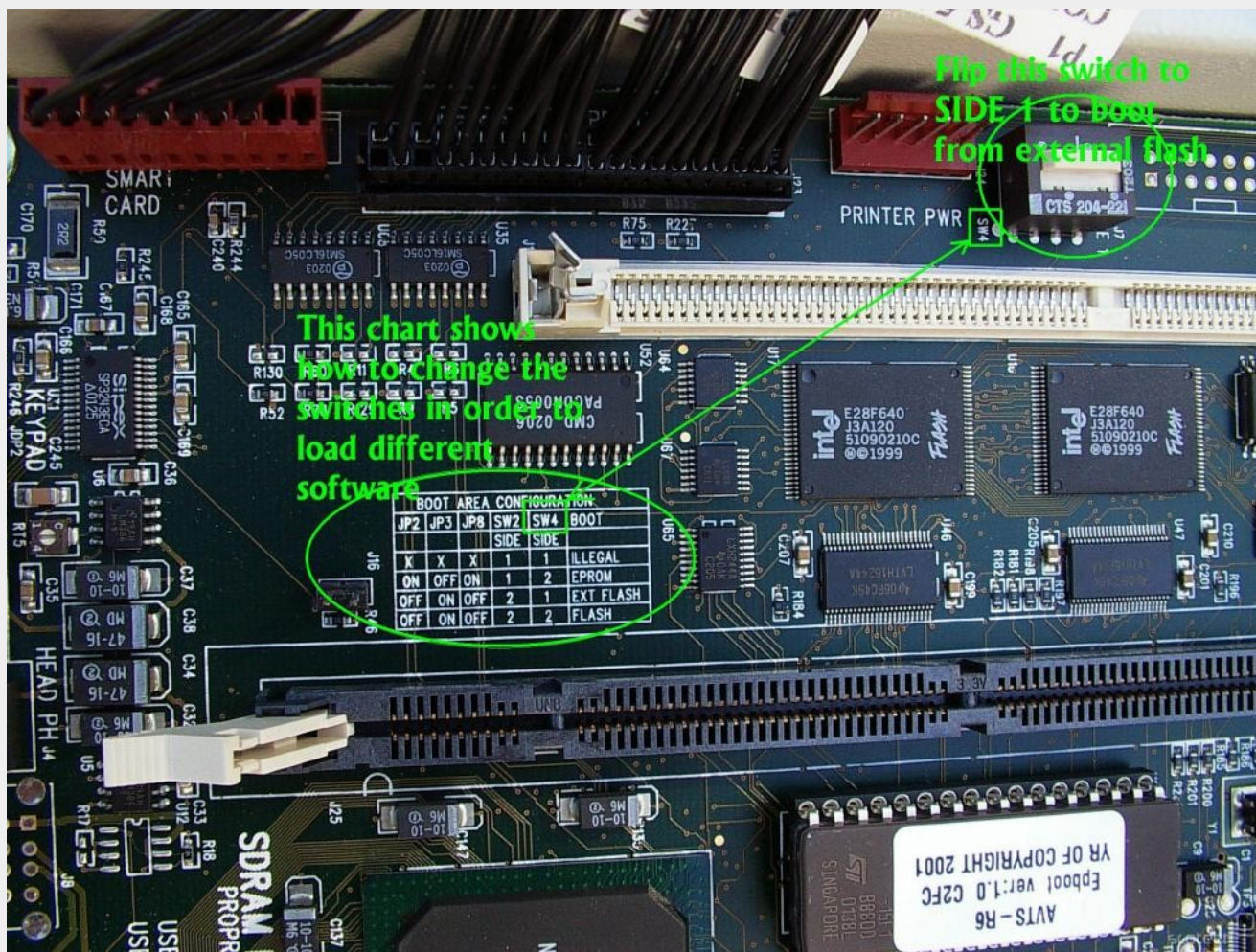
Transparentnost tehnologije, dostop do kode programa?

Varnost v praksi

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
ACLogic CesarFTP 0.98b, 0.99 g, 0.99 e	A buffer overflow vulnerability exists during authentication due to insufficient bounds checking, which could let a remote user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit script has been published.	CesarFTP Buffer Overflow	Low/High (High if arbitrary code can be executed)	Securiteam, August 31, 2003
Comersus Open Technologies Comersus Cart 5.0 991	A vulnerability exists in the 'comersus_customerLoggedVerify.asp' script due to insufficient validation of the 'redirecturl' parameter, which could let a remote malicious user obtain or modify sensitive information or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Comersus Shopping Cart 'redirecturl' Input Validation	Medium/High (High if arbitrary code can be executed)	SecurityTracker Alert ID: 1011135, September 1, 2004
Diebold GEMS Central Tabulator 1.17.7, 1.18	A vulnerability exists due to an undocumented backdoor account, which could a local or remote authenticated malicious user modify votes. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	GEMS Central Tabulator Vote Database Vote Modification	Medium	BlackBoxVoting.org, August 31, 2004
IPSwitch IMail 5.0, 5.0.5-5.0.8, 6.0-6.0.6, 6.1-6.4, 7.0.1-7.0.7, 7.1, 7.12, 8.0.3, 8.0.5, 8.1	Multiple buffer overflow vulnerabilities exist: a remote Denial of Service vulnerability exists in the Queue Manager when a malicious user submits an overly long sender field; a remote Denial of Service vulnerability exists in Web Calendaring when a calendar entry that contains certain content is viewed; and a remote Denial of Service vulnerability exists in Web Messaging when a malicious user submits an overly long 'To:' line. The execution of arbitrary code may also be possible. Patches available at: http://www.ipswitch.com/support/imap/releases/imap_professional/im813.html We are not aware of any exploits for this vulnerability.	IPswitch IMail Server Multiple Buffer Overflow Remote Denial of Service	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA12453, September 3, 2004

CERT-ovo opozorilo o nedokumentiranem uporabniškem računu v Dieboldovih volilnih napravah. Vir: Spletna stran CERT.

Varnost v praksi



Prilagoditev Dieboldovih volilnih naprav. Pri OpenVotingFoundation.org so avgusta 2006 odkrili kako v štirih minutah prilagoditi Dieboldovo volilno napravo Accuvote TS, da omogoča poganjanje neavtorizirane programske opreme. Vir: Open Voting Foundation.

Varnost v praksi



Prikaz varnostnih ranljivosti v Dieboldovi volilni napravi Accuvote TS. Analiza je bila opravljena pa Princetonski univerzi v ZDA.

Vir: Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten (2006): Security Analysis of the Diebold AccuVote-TS Voting Machine, <<http://itpolicy.princeton.edu/voting/>>

Varnost v praksi



Vulnerability Assessment Team at Argonne National Laboratory in Illinois, 2011, <<http://www.bradblog.com/?p=8785>>, <<http://www.ne.anl.gov/capabilities/vat/election-security/>>.

Varnost v praksi



Skupini Wij vertrouwen stemcomputers niet ter Chaos Computer Club sta leta 2006 prikazali kako je mogoče ponarejati e-volitve ob uporabi Nedapovih volilnih naprav (tim. Nedap PowerFraud izveden na volilni napravi Nedap/Groenendaal ES3B), s preprosto menjavo dveh EPROM čipov. Oktobra 2006 so zaradi odkritih ranljivosti uporabo teh elektronskih volilnih naprav na Nizozemskem prepovedali.

Vir in avtorstvo: Wij vertrouwen stemcomputers niet ter CCC,
<<http://www.wijvertrouwenstemcomputersniet.nl/Nedap-en>>

Video: <<http://chaosradio.ccc.de/media/video/2006-10-04-nl-eenvandaag-stemcomputers-subtitles.mp4>>.

Video: Changing the ROMs of a Nedap e-voting computer in 60 seconds,
<<http://www.youtube.com/watch?v=EowKaIRT3lc>>.

Varnost v praksi

voting computer tempest attack



Tempest napad na volilne naprave na Nizozemskem leta 2006. Z analizo elektromagnetnega sevanja je mogoče kršiti volilno tajnost. Oktobra 2006 so zaradi odkritih ranljivosti uporabo teh elektronskih volilnih naprav prepovedali.

Vir in avtorstvo: Wels, Wessling, Gonggrijp in Németh, organizacija "We don't trust voting computers", <<http://www.wijvertrouwenstemcomputersniet.nl/English>>

Video na YouTube: <<http://www.youtube.com/watch?v=B05wPomCjEY>>.

Varnost v praksi



Skupina raziskovalcev iz IndiaEVM.org (J. Alex Halderman, Hari K. Prasad in Rop Gonggrijp) je leta 2010 opravila varnostno analizo indijskih volilnih naprav. Pokazali so celo kako je želeni izid volitev mogoče "nastaviti" kar preko Bluetooth povezave s pomočjo mobilnega telefona. (Vir: <<http://indiaevm.org/>>.)

Varnost v praksi

Brazilska vlada je 10. do 13. novembra 2009 ("cele" 3 dni!) izvajala test sistema za elektronsko glasovanje. Konec novembra 2009 pa je Sergio Freitas da Silva uspel zlomiti tajnost glasovanja s pomočjo Tempest napada.

Oktobra 2007 je nizozemsko okrožno sodišče v Amsterdamu prepovedalo uporabo volilnih naprav, maja 2008 pa se je nizozemska vlada odločila, da bodo v bodoče na Nizozemskem volitve potekale zgolj na klasičen način.

Nemško ustavno sodišče je 3. marca 2009 presodilo, da je uporaba elektronskih volilnih naprav na splošnih volitvah neustavna, saj obstoječe volilne naprave ne dosegaajo ustavnih zahtev glede tajnosti volitev.

Predlogi za izboljšanje varnosti

Številni varnostni problemi že pri elektronskih volitvah na volišču.

Predlogi za izboljšanje varnosti:

- Rebecca Mercuri - Voter Verified Paper Audit Trail (Mercuri method).
- Avstralija je leta 2001 izvedla e-volitve na odprtokodnem sistem EVACS, ki temelji na Linuxu.

Elektronske volitve v Sloveniji

Študija Grad, Franci, Lukšič, Andrej in Zagorc, Saša. Študija izvedljivosti e-volitev s predlogi implementacije, 2004.

Novela Zakona o volitvah v državni zbor iz julija 2006 je v 79.a členu določila, da okrajna volilna komisija za območje okraja določi najmanj eno volišče, ki je dostopno invalidom, na tem volišču pa lahko volilna komisija omogoči glasovanje s posebej prilagojenimi glasovnicami in **glasovalnimi stroji**.

Volilne naprave TopVoter je pričelo ponujati slovensko podjetje.

Prvič so bili glasovalni stroji uporabljeni oktobra 2006 na lokalnih volitvah.

Elektronske volitve v Sloveniji

Glasovalne naprave | TopVoter
 volilne naprave - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://www.topvoter.com/

ISG TopVoter volilne naprave

TIPI NAPRAV POGOSTA VPRAŠANJA IN ODGOVORI IZJAVA O EKSKLUZIVNOSTI MNENJA

NAPRAVE
Topvoter Basic
Topvoter Touch
Enostavno kot uporaba bančnega avtomata!
Topvoter Sound
Tudi za slepe in nepismene!

Glasovalne naprave

MEDJI
Pogovor na radiju Sora
E-volitve bodo možne tudi v Murski Soboti (SOBOTAINFO, 3.10.06)
Elektronsko glasovanje le v peščici občin (Večer, 3.10.06)
Prvič tudi elektronske glasovnice (TV Slovenija, 2.10.06)
Invalidi bodo lažje oddajali svoj glas (Delo, 6.10.06)

več

Končano Anonimizacija izključena Adblock

Spletna stran naprav TopVoter, <http://www.topvoter.com/>

Elektronske volitve v Sloveniji

Naprava omogoča glasovanje preko zaslona na dotik ter natisne glasovalni listič (tim. *Voter Verified Paper Audit Trail*).

Na vprašanje v zvezi s tem so pri podjetju odgovorili, da je "tiskanje namenjeno le kasnejši kontroli (če bi bila potrebna) ali pa za primer večje okvare naprave - v tem primeru se uporabijo natisnane glasovnice na klasičen način".

Odgovor predstavnika podjetja glede podrobnejših informacij in varnosti (nekaj dni pred lokalnimi volitvami 2006):

"Žal imamo v teh dneh premalo časa za zelo podrobne informacije. Lahko povem, da smo zasnovali lastno rešitev (ne odprtokodno), ki pa temelji na Linuxu. Zakaj Linux, vam verjetno ni potrebno razlagati, saj so vam prednosti Linuxa poznane. Aplikacija je razvita v Javi. Kar se tiče varnosti jo zagotavljamo na več nivojih, jasno pa da podrobnosti ne smemo objavljati.

...

Verjetno bi vas zanimalo še veliko podrobnosti, žal pa mi čas tega ne dopušča."

Volitve preko interneta?

Gre pri internetnih volitvah res zgolj za spremembo "medija" oz. infrastrukture?

Ali morda sprememba "medija" za sabo potegne tudi spremembo samega koncepta glasovanja?

Zahteve volitev:

- splošne,
- svobodne (brez oglasov, zavestno nepravilno glasovanje),
- enakopravne (en volivec – en glas),
- tajne (uravnoteženost tajnosti in transparentnosti; naj ne omogoča preprodaje glasov (npr. z možnostjo izpisa potrdila, ki potrjuje kako je volivec glasoval))
- neposredne (brez posrednikov).

Tehnični in družbeni problemi!

Internetne volitve v Sloveniji

Sistem "dvojnih elektronskih ovojnica".

Problem varnega volilnega okolja.

Problem varnosti terminalne opreme uporabnika.

Tajnost glasovanja se doseže z anonimizacijo, ne zagotavlja pa je sistem kot tak.

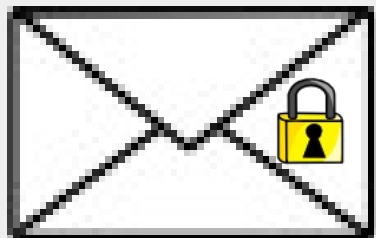
Bo delež volivcev narasel?

Elektronske storitve in internetno glasovanje – dva različna problema.

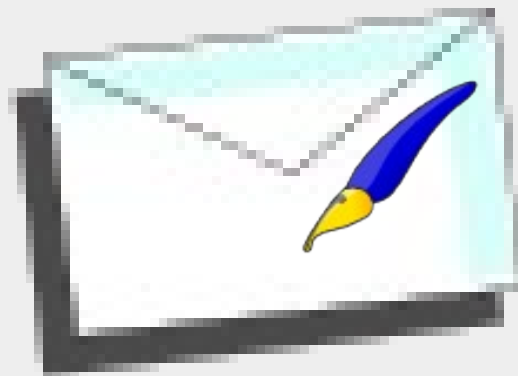
Odprta koda: da ali ne?

Prvi predlog pripravljen leta 2007, vendar kasneje opuščen.

Internetne volitve v Sloveniji



Glasovnica je shranjena
v prvi, šifrirani
"elektronski ovojnici"...



...ter se "vstavi" v drugo,
ki je digitalno podpisana
in vsebuje ime volivca
ter časovni žig

Internetne volitve v Sloveniji



Prvi volilni strežnik preveri digitalne podpise volivcev (ali imajo volilno pravico ter izloči morebitne prejšnje glasovnice istega volivca)



Drugi, ločen volilni strežnik dešifrira glasovnice ter ugotovi rezultat.

Razlogi za internetne volitve

Hitrejše in bolj natančno štetje glasovnic, na dolgi rok nižja cena izvedbe glasovanja.

Internetne volitve so "in": večja učinkovitost, modernizacija glasovalnega procesa, gre za nadaljevanje informatizacije vseh ostalih storitev, vlada in politika se skušata predstaviti kot moderni oz. se želimo uveljaviti kot e-nacija,...

Internetne volitve so pripomoček, ki lahko zaustavi trende upada zanimanja za volitve in za demokratični proces: dvig volilne udeležbe, olajšan dostop do volišča naj bi okrepil in izboljšal demokratični proces.

Povečanje volilne udeležbe

Tiha predpostavka: pomemben ali celo bistven razlog za upad volilne udeležbe naj bi bilo dejstvo, da se volivcem ne ljubi hoditi na volišče. (???)

Ali internetni dostop do volišča vpliva na povečanje volilne udeležbe?

*Poročilo ženevskega kantona o elektronskih volitvah iz julija 2007 na strani 2 navaja podatek, da je bil v Švici odstotek internetnih volivcev med leti od 2002 do 2006 na osmih volitvah redno okrog 20%, med temi dvajsetimi odstotki pa je bilo med 5 do 10% takšnih volivcev, ki prej niso volili. **To v celotni populaciji pomeni 1 do 2% povečano volilno udeležbo, kar je razmeroma malo.***

Povečanje volilne udeležbe

Estonija 2007: elektronsko je preko interneta svoj glas na volitvah oddalo 3,4% vseh, ki so volili (leta 2009 pri volitvah v Evropski parlament že 15,7). Podatkov o "novih" volivcih pa ni bilo.

1992: 67,84%

1995: 69,06% (↗ +1,22)

1999: 57,43% (↘ -11,63)

2003: 58,20% (↗ +0,77)

2007: 61,91% (↗ +3,71)

V Estoniji je imelo pametne kartice s certifikati 90% volilnih upravičencev, imeli so pet let izkušenj s karticami.

V Sloveniji je leta 2006 imelo digitalna potrdila manj kot manj kot 10% volilnih upravičencev.

E-storive vs. internetno glasovanje

Gre za dva različna problema.

Pri elektronskem poslovanju se varnost transakcij zagotavlja z zagotavljanjem istovetnosti in preverjanjem identitete.

“Finančnim transakcijam so priložena imena: kdo dobi denar, kdo ga izgubi. Glasovnice nosijo le informacijo o prejemniku: celoten smisel tajne glasovnice je v tem, da se odstrani ime volivca. Zaradi tega je sistem veliko težje zaščititi pred zlorabo, veliko težje je ugotoviti zlorabo, če do nje pride in veliko težje je identificirati napadalca in ga zapreti” (Schneier, 2001 - Internet Voting vs. Large-Value e-Commerce).

E-storive vs. internetno glasovanje

Gre za drugačen tip varnostnega problema.

Varnost elektronskih finančnih transakcij je zagotovljena z zmožnostjo revizije izvedenih transakcij, ki je mogoča zaradi identifikacijskih podatkov.

Pri uporabi informacijsko komunikacijske tehnologije za namene internetnih volitev gre za netipično uporabo te tehnologije.

Različna pogostost uporabe tehnologije za izvajanje finančnih transakcij ter elektronskih volitev.

“Volilni sistemi so v uporabi redko, največ nekajkrat na leto. Sistemi, ki so v uporabi vsak dan se izboljšujejo, ker ljudje nanje postanejo navajeni, odkrijejo napake in se spomnijo izboljšav.” (Schneier, 2004 - Getting Out the Vote: Why is it so hard to run an honest election?).

Manjša transparentnost

Za razumevanje “delovanja” klasične volilne skrinjice ni potrebno praktično nikakršno predznanje.

Povprečen volivec, član volilnega odbora ali zaupnik na volišču pa **nima ustreznega znanja** za podrobno razumevanje delovanja sodobnih komunikacijsko informacijskih sistemov.

Ti sistemi so **kompleksni**, kar jim zmanjšuje **transparentnost** pa tudi samo varnost.

Elektronski volilni sistem je za povprečnega posameznika v bistvu “črna škatla”.

Zagotavljanje anonimnosti

Elektronski volilni imenik – vsebuje podatke o tem, kdo je volil.

Sistem “dvojnih elektronskih ovojníc” sam po sebi ne zagotavlja anonimnosti. Tajnost glasovanja dosežemo z **anonimizacijo glasovnic**.

Vprašanje **zaupanja** v posestnika šifrirnega ključa oziroma upravitelja informacijsko komunikacijskega sistema!

Uporaba nove tehnologije odpira nove probleme, ki pa jih ne rešujemo s tehnologijo, pač pa z **dodatnimi pravnimi in organizacijskimi pravili**.

Varno volilno okolje?

Varnost terminalne opreme uporabnikov?

Volilni molk (ob bolj razširjenem internetnem glasovanju)?

Če volišče "preselimo" v dnevno sobo, odgovornost za zagotovitev varnega volilnega okolja država **preloži** na volivca.

Možnosti za preprodajo glasov, volivec lahko dokaže kako je volil, lahko pride do kršitev tajnosti glasovanja (opazovanje volivca), zloraba digitalnega potrdila (umrle osebe, ne-volivci)...

Varno volilno okolje?

Uvedba nove tehnologije je odprla nove možnosti zlorab, te nove probleme pa zopet ne rešujemo s tehnologijo, pač pa s pravnimi in organizacijskimi pravili.

Predlagani sistem, ki opredeljuje možnost večkratnega elektronskega in v končni fazi še klasičnega glasovanja, že v osnovi skuša reševati zgolj problem **odkritih pritiskov** na volivca, ne pa tudi problema **prikrite kršitve volilne tajnosti**.

Nadaljevanje ideje o glasovanju po pošti?

Po pošti lahko glasujejo:

- osebe, ki so na zdravljenju v bolnišnicah;
- oskrbovanci domov za starejše, ki nimajo stalnega prebivališča v domu;
- volivci, ki so na dan glasovanja v tujini.

Volitev po pošti se udeležuje le **omejen krog ljudi**, poleg tega gre za **izjemo**, ki glasovanje omogoča posebnim, deprivilegiranim skupinam.

Pri internetnih volitvah princip glasovanja in nekontroliranega volilnega okolja potencialno prenašamo **na celotno populacijo volivcev**.

Ocena smiselnosti uvedbe (2007)

1. Kaj skušamo doseči oz. izboljšati z uvedbo internetnih volitev?

Z uvedbo internetnih volitev skušamo izboljšati sistem glasovanja, povečati volilno udeležbo in posledično izboljšati demokracijo. Skušamo se tudi predstaviti kot moderna država.

2. Katere so težave z obstoječim načinom glasovanja?

Zagovorniki uvedbe internetnih volitev navajajo dva sklopa težav: padanje volilne udeležbe in zanimanja za demokracijo ter dejstvo, da so klasične volitve staromodne (da je potrebno volilni proces modernizirati, itd.).

Ocena smiselnosti uvedbe (2007)

3. Kako dobro uvedba internetnih volitev lajša te težave?

Uvedba internetnih volitev po eni strani omogoča, da volivec glasuje od doma in se mu ni treba sprehoditi do volišča, kar v teoriji lahko dvigne volilno udeležbo.

Projekt internetnih volitev pomeni tudi dobro promocijo tako za državo, kot za njeno politiko.

4. Katere težave povzroča uporaba internetnih volitev?

Anonimnost ni več vgrajena v sistem, pač pa jo je potrebno zagotoviti z anonimizacijo. Država volivcu ne zagotavlja več varnega volilnega okolja. Manjša transparentnost sistema...

Ocena smiselnosti uvedbe (2007)

5. Kakšne dileme in kakšno tehtanje (ang. *trade-off*) predpostavlja uvedba internetnih volitev?

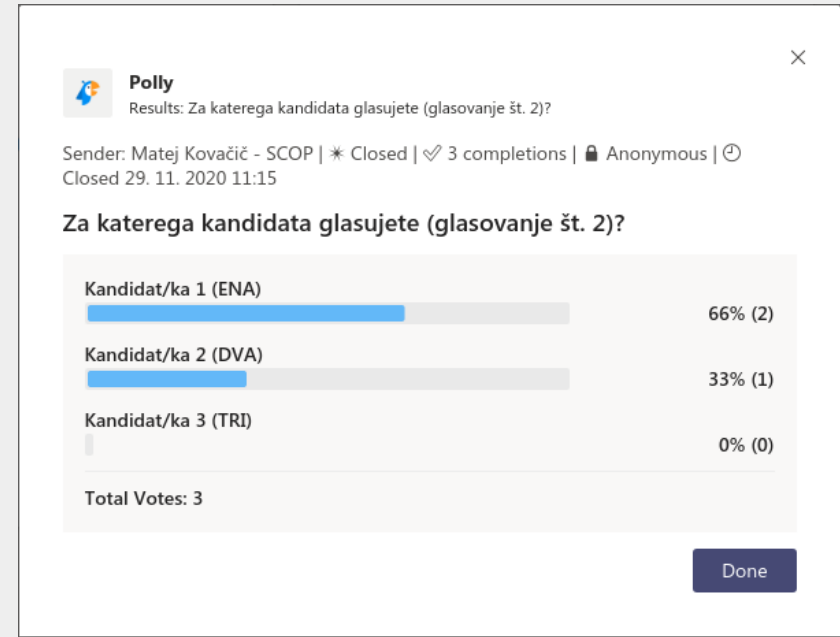
Po eni strani z uvedbo internetnih volitev pridobimo možnost večje udobnosti pri glasovanju, (malenkostno) se poveča volilna udeležba, projekt pa je dobra promocija za državo in njeno politiko.

Po drugi strani pridobimo več potencialnih varnostnih ranljivosti in sistem, ki v osnovi ne zagotavlja tajnosti glasovanja, pač pa so za le-to potrebna dodatna pravna in organizacijska pravila.

Forenzična analiza e-volilnega sistema

Na podlagi zaprosila VSS Sindikata UM smo sodelavci Inštituta za forenziko informacijskih tehnologij novembra 2020 opravili forenzični pregled sistema elektronskih volitev

s sistemom Polly v okolju MS Teams, ki ga je implementirala Univerza v Mariboru za glasovanja o kandidatih za izvolitve v nazive na videokonferenčnih sejah senata.



Forenzična analiza e-volilnega sistema

Ugotovitve:

- Sklicatelj volitev lahko med potekom volitev vidi, kako poteka glasovanje in kakšno je razmerje glasov.
- Sklicatelj volitev v določenih okoliščinah lahko poveže vsebino glasovnice z volivcem.
- Sistem ne omogoča, da bi bili podatki skrbno varovani in tajni vse do štetja glasov, saj ne vsebuje nikakršnih kriptografskih mehanizmov za zagotavljanje oz. preverjanje integritete oddanih glasovnic.

Forenzična analiza e-volilnega sistema

Ugotovitve:

- Sistem meri ne preprečuje možnosti spreminjanja že oddanih glasov v dovoljšnji meri.
- Zbrani podatki se hranijo v oblaknih storitvah ponudnikov iz ZDA, kar je v določenih primerih lahko pravno sporno.
- E-volilni sistemi ne omogočajo zagotavljanja kontroliranega volilnega okolja, ki ga lahko zagotovijo le klasične volitve.

Forenzična analiza e-volilnega sistema

Sklep:

V kolikor uporabniki nimajo težav glede že omenjenih pomislekov, tako z vidika tajnosti, kot tudi zaupnosti ipd., bi ga lahko uporabili tudi kot orodje za izvedbo volitev. Vendar pa, kot je bilo že omenjeno, vtičnik temu ni namenjen in z vidika resnih volitev, ne dosega potrebnih standardov.

Volitive in blockchain?

Why is blockchain voting a dumb idea? Glad you asked.

For starters:

- It doesn't solve any problems civil elections actually have.
- It's basically incompatible with "software independence", considered an essential property.
- It can make ballot secrecy difficult or impossible.

-- Matt Blaze (american researcher who focuses on the areas of secure systems, cryptography, and trust management).

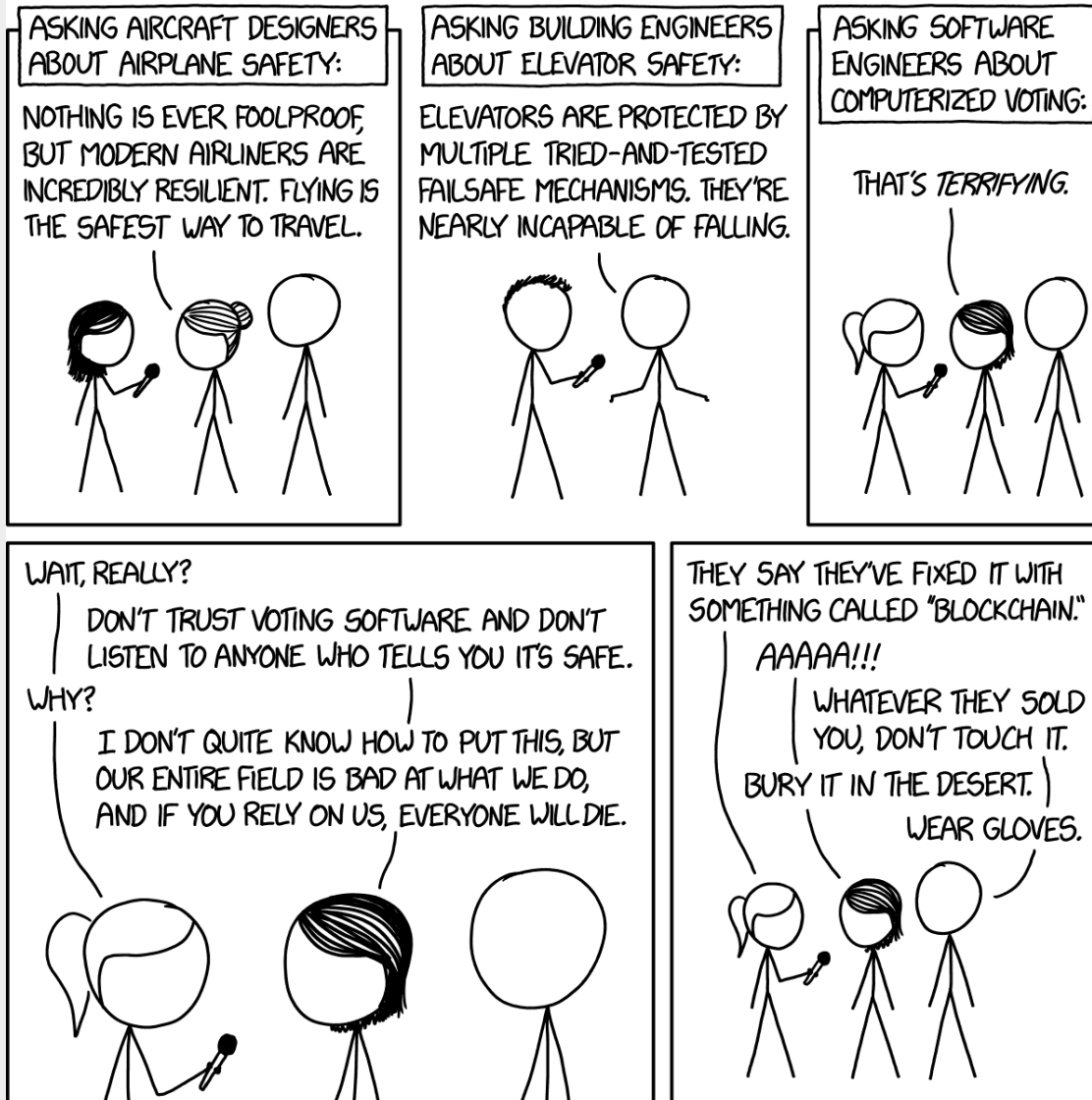
Volitive in blockchain?

»This article examines the suggestions that “voting over the Internet” or “voting on the blockchain” would increase election security, and finds such claims to be wanting and **misleading**. ... Internet- and blockchain-based voting would **greatly increase the risk of undetectable, nation-scale election failures**. ... However, studies have been inconclusive, showing that online voting may have **little to no effect on turnout in practice**, and it may even increase disenfranchisement. More importantly: given the current state of computer security, any turnout increase derived from with Internet- or blockchain-based voting would come at the cost of losing meaningful assurance that votes have been counted as they were cast, and not undetectably altered or discarded.«

Park, Specter, Narula, Rivest. 2020. Going from Bad to Worse: From Internet Voting to Blockchain Voting.

<https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf>

Volitive in blockchain?



Vprašanja?



Matej Kovačič

<https://telefoncek.si>



This work is published under
CC BY-NC-SA 4.0 license