

Informacijsko varnostni vidiki e-volitev

Infosek 2007, 23. november 2007

Matej Kovačič, Jožko Škrablin
Fakulteta za družbene vede

(CC) 2007

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Streliška 1, 1000 Ljubljana.

E-volitve, i-volitve...

- Elektronsko štetje klasično oddanih glasovnic / oddaja elektronske glasovnice.
- Glasovanje na volišču / glasovanje na daljavo.
- **Elektronske volitve** (e-volitve): volilci lahko glasujejo s pomočjo elektronske naprave na klasičnem volišču (lahko kateremkoli).
- **Internetne volitve** (i-volitve): volilci lahko glasujejo preko interneta. Volilci obišejo posebno volilno spletno stran, kjer se elektronsko identificirajo in oddajo svoj glas.
- Za volilce je verjetno enostavnejša izvedba e-volitev, kot i-volitev: bankomati vs. internet.

E-volitve



Volina naprava v Braziliji, foto: Antonio Cruz/ABr, Creative Commons Attribution 2.5 Brazil



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

Razmislek o varnosti na splošno...

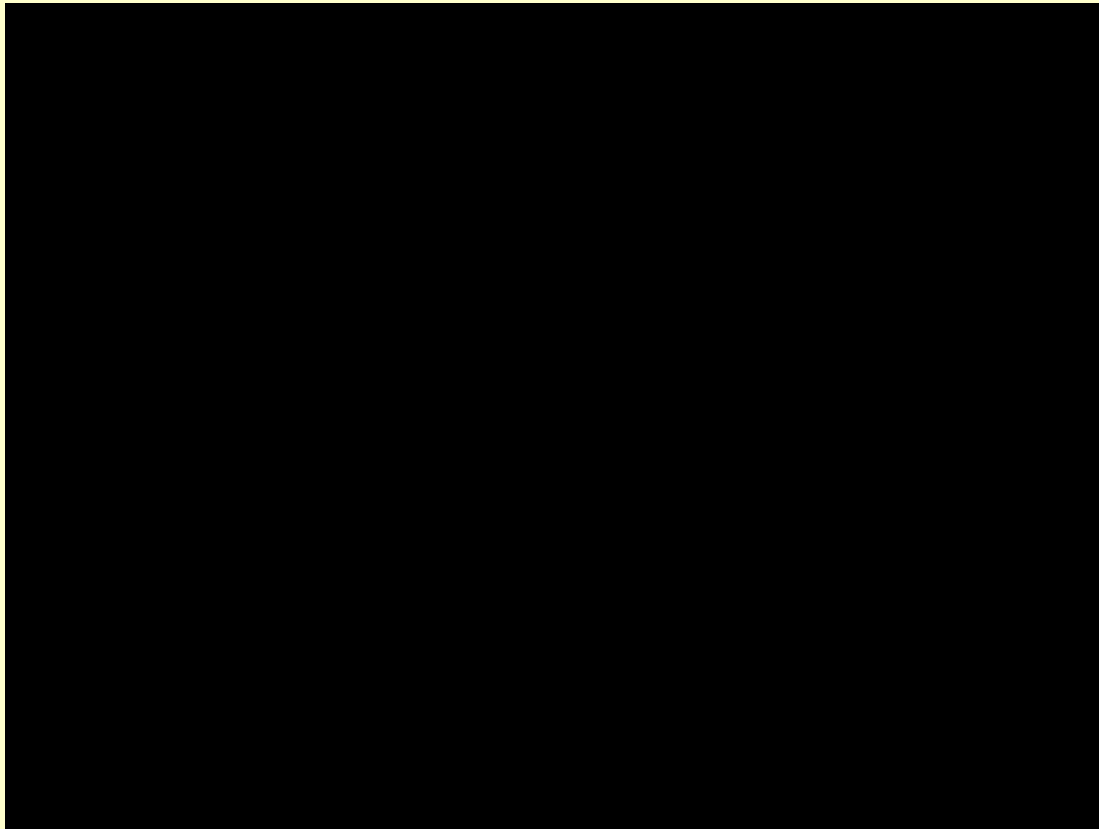
- Gre za varovanje elektronskih glasovnic pred nepooblaščenim dostopom, uporabo, razkritjem, uničenjem, spreminjanjem ali izgubo.
- Gre tudi za varovanje zasebnosti volilca in zagotavljanje tajnosti glasovanja.
- Glasovalne naprave – ali glasovalni računalniki?
- Kraja klasičnih volitev zahteva široko zaroto, kaj pa kraja elektronskih volitev?
- *Single point of failure* pri sistemu i-volitev?
- Transparentnost tehnologije, dostop do kode programa?

Varnost e-volitev

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/imap813.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 e-volitev



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 e-volitev



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 e-volitev

- Številni varnostni problemi že pri e-volitvah.
- 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

- 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

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

Varnost TopVoter naprav?

- 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 natiskane glasovnice na klasičen način*".

Varnost TopVoter naprav?

- 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.”

Varnost TopVoter naprav?

- 17. septembra smo na upravo podjetja poslali pisno zaprosilo za podrobnejši pregled naprav (s povratnico), vendar je bila pošiljka zaradi napačnega naslova zavrnjena (naslov smo dobili na spletni strani).
- 21. septembra 2007 smo predstavniku podjetja na drugi naslov poslali pisno zaprosilo za podrobnejši pregled naprav (s povratnico).
- Odgovora nismo prejeli.
- 1. oktobra smo jim zaprosilo poslali po elektronski pošti in dobili odgovor, da nam bodo odgovorili takoj, ko bo mogoče.
- Državna volilna komisija ni predpisala postopkov cetrifikacije volilnih naprav.

Kaj pa i-volitve?

- Gre pri i-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 volilec – en glas),
 - tajne (uravnoteženost tajnosti in transparentnosti; naj ne omogoča preprodaje glasov (npr. z možnostjo izpisa potrdila, ki potrjuje kako je volilec glasoval))
 - neposredne (brez posrednikov).
- **Tehnični in *družbeni* problemi!**

Razlogi za i-volitve

- Hitrejše in bolj natančno štetje glasovnic, na dolgi rok nižja cena izvedbe glasovanja.
- **I-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,...
- **I-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 volilcem 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 i-volilcev med leti od 2002 do 2006 na osmih volitvah redno okrog 20%, med temi dvajsetimi odstotki pa je bilo med 5 do 10% takšnih volilcev, 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. Podatkov o "novih" volilcih pa ni.

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 ima pametne kartice s certifikati 90% volilnih upravičencev. Pet let izkušenj s karticami.
- V Sloveniji je leta 2006 imelo digitalne certifikate le dobrih 36% aktivnih mesečnih uporabnikov interneta, SIGEN-CA manj kot 10%.

Elektronske storitve in internetno glasovanje – 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 volilca. 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).

Elektronske storitve in internetno glasovanje – dva različna problema

- 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 i-volitev gre za **netipično uporabo te tehnologije**.
- + Obvezna hramba prometnih podatkov (*Zakon o elektronskih komunikacijah*, člani 107 do 107. e).

Elektronske storitve in internetno glasovanje – dva različna problema

- **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?).

Sistem i-volitev ni transparenten

- Za razumevanje "delovanja" klasične volilne skrinjice ni potrebno praktično nikakršno predznanje.
- Povprečen volilec, 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**".

Sistem i-volitev ne zagotavlja anonimnosti sam po sebi

- 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**.

Pri internetnih volitvah volilcu ni zagotovljeno varno volilno okolje

- Varnost terminalne opreme uporabnikov?
- Volilni molk (ob bolj razširjenem i-glasovanju)?
- Če volišče "preselimo" v dnevno sobo, odgovornost za zagotovitev varnega volilnega okolja država **preloži** na volilca.
- Možnosti za preprodajo glasov, volilec lahko dokaže kako je volil, lahko pride do kršitev tajnosti glasovanja (opazovanje volilca), zloraba digitalnega certifikata (umrle osebe, nevolilci)...

Pri internetnih volitvah volilcu ni zagotovljeno 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 volilca, ne pa tudi problema **prikrite kršitve volilne tajnosti**.

Kaj ne gre pri i-volitvah le za 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;
 - volilci, 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 i-volitvah princip glasovanja in nekontroliranega volilnega okolja potencialno prenašamo na **celotno populacijo volilcev**.

Ocena učinkovitosti in smiselnosti uvajanja i-volitev

1. Kaj skušamo zaščititi oz. izboljšati z uvedbo i-volitev?
2. Katere so težave z obstoječim načinom glasovanja?
3. Kako dobro uvedba i-volitev lajša te težave?
4. Katere težave povzroča uporaba i-volitev?
5. Kakšne dileme in kakšno tehtanje (ang. *trade-off*) predpostavlja uvedba i-volitev?

Ocena učinkovitosti i-volitev

1. Kaj skušamo doseči oz. izboljšati z uvedbo i-volitev?

- Z uvedbo i-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 i-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 učinkovitosti i-volitev

3. Kako dobro uvedba i-volitev lajša te težave?

- Uvedba i-volitev po eni strani omogoča, da volilec glasuje od doma in se mu ni treba sprehoditi do volišča, kar v teoriji lahko dvigne volilno udeležbo.
- Projekt i-volitev pomeni tudi dobro promocijo tako za državo, kot za njeno politiko.

4. Katere težave povzroča uporaba i-volitev?

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

Ocena učinkovitosti i-volitev

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

- Po eni strani z uvedbo i-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.

Zaključek?

- Nova tehnologija prinaša nove varnostne probleme.

Ali uvedba i-volitev res prinaša veliko dodano vrednost?

<http://www.elektronske-volitve.si>