Simon Anikó

Elektronikus szavazórendszerek megoldásainak elemzése, bemutatása

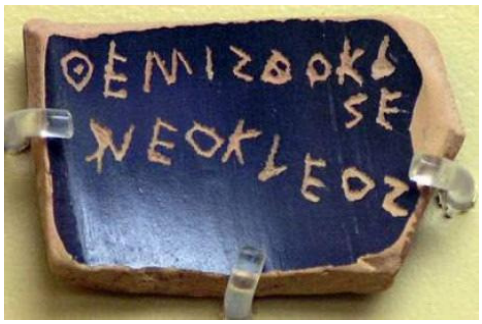
21. téma

Tartalomjegyzék

1 Bevezető

Amióta létezik demokrácia, és nem egy szűk politikai csoport, esetleg egyetlen fő hozhat döntést tömegeket érintő kérdésekben, azóta szükség van egy olyan módszerre, amellyel az emberek sokaságának megfelelő döntést meg lehet hozni. Ez a módszer a szavazás.

Szavazással sok helyen találkozhatunk ha a történelmi könyveinket lapozgatjuk. Egyik nevezetes változata az ókori görögöknél létezett: a cserépszavazás (más nevén osztrakiszmosz). Egy olyan szavazási formáról van szó, amely névtelenül zajlott. Használatával lehetősége nyílt a városállam polgárainak arra, hogy egy –az államra nézve általuk veszélyesnek ítélt-, befolyásos személyt száműzzenek 10 évre. A szavazáshoz törött cserépdarabokat (ún. osztrakon, lásd 1. ábra) használtak és arra írták a száműzendő személy nevét. [1.]



1. ábra: Egy szavazásra használt cserépdarab (osztrakon)
Themisztoklész nevével

A szavazási, választási módszerek hosszú időn keresztül csak papír alapúak voltak. Sok helyen a fontosabb kérdésekben (például parlamenti választások) még mindig ilyen úton történik a választópolgárok szavazatainak rögzítése. Ám ne feledkezzünk meg arról, hogy manapság a technika valamint az Internet segítségével olyan új lehetőségek is szóba jöhetnek a szavazások/véleménynyilvánítások terén, amelyek korábban nem voltak elképzelhetőek. Gondoljunk például a néhány óra alatt lebonyolított szavazásokra, ahol a közönség véleményét kérik ki a különböző tévéműsorokban; vagy a közösségi oldalakon szervezett változataira, ahol a voksolók tetszését elnyerők akár értékes díjakat kaphatnak. Ezekben az esetekben nem fontos annak biztosítása, hogy mindenki csak egy érvényes szavazatot tegyen, továbbá a névtelenség sem kritikus kérdés, de a felgyorsult világ elvárásaira (pl. gyors lebonyolítás, kis komplikáltság stb.) jó példát nyújthatnak.

A továbbiakban főként az elektronikus szavazórendszerekkel fogok foglalkozni, ahol egy sor feltételnek kell eleget tennie a különböző megoldásoknak. Az ezekkel a rendszerekkel szemben támasztott követelményeket és néhány gyakorlati megvalósítást fogok bemutatni a következő részekben.

2 Elektronikus szavazás és szavazórendszerek

2.1 Az elektronikus szavazás és tulajdonságai

[2.] Ha elektronikus szavazásról beszélünk, akkor a szavazatok elektronikus leadását és azok elektronikus összeszámlálását értjük alatta.

Alapvetően két változata képzelhető el:

- Az első esetben a szavazás menetét megbízottak, felügyelők (pl. az állam által kiküldött személyek) követik figyelemmel. Ebben az esetben a szavazás -a hagyományos rendszerekhez hasonlóan-, előre kijelölt helyeken zajlik.
- A második eset a távoli szavazás (remote e-voting), amikor a szavazást nem követik figyelemmel megbízottak, az egész folyamat csak a felhasználó befolyása alatt van. Ilyen lehet például, amikor az adott személy a számítógépéről, mobiltelefonjáról vagy az Interneten keresztül szavaz.

Az elektronikus szavazás több előnnyel is rendelkezik a hagyományos módszerekhez képest. Míg a papír alapú szavazásoknál órákon keresztül eltarthat a szavazatok számlálása (és előfordulhatnak számolási hibák is), addig az elektronikus szavazórendszerek esetén a számlálás nagyon *gyors*an és *pontos*an elvégezhető. A résztvevők szempontjából nem elhanyagolható tulajdonság a *kényelem* (például otthonról voksolnak az emberek, vagy az elektronikus szavazást lebonyolító gép több nyelven is biztosítja a kitöltendő űrlapot). Ez a tulajdonság maga után vonhatja a nagyobb részvételi arányt, szavazási hajlandóságot is. Arról se feledkezzünk meg, hogy a szavazás ebben a formában elérhetőbbé válik a fogyatékkal élők számára, ráadásul *kisebb költség*gel jár, mint a hagyományos szavazási módszerek (pl. nincs szükség szavazólap/űrlap nyomtatására).

Hátrányt jelenthetnek egy ilyen rendszer beüzemelésével kapcsolatos kiadások, amelyek néha többe kerülhetnek, mint a szavazati űrlapok nyomtatása és hagyományos szavazás lebonyolítása.

A korábban taglalt tulajdonságokon túlmenően azonban nem téveszthetjük szem elől a biztonság, ellenőrizhetőség (verifiability) és a privátszféra kérdéseit sem.

Ha a biztonságot tekintjük, akkor a szavazórendszer szoftverének megbízható forrásból kell származnia és rendeltetésszerűen kell működnie. A megfelelő működéshez hozzátartozik például annak biztosítása, hogy a szavazóűrlapok úgy jelennek meg a terminálok kijelzőjén, ahogyan majd a rendszer a szavazatokat rögzíteni fogja (tehát ha a rendszer csak azt rögzíti, hogy a második jelöltre érkezett voks, akkor a rendszerben tárolt és a kijelzőn megjelenő második jelöltnek ugyanannak kell lennie). Ennek egy lehetséges ellenőrzési módszere az, hogy a szavazóterminál a szavazás végén nyomtat egy cédulát, amin szerepelnek a rögzített adatok. Így a választó meggyőződhet arról, hogy döntése helyesen lett felvéve. Amúgy ez a módszer a VVPAT (Voter Verified Paper Audit Trail), amelyhez kötődően további kérdések merültek fel [4.]. Ilyen kérdéses dolog, hogy a szavazás lezárása után a kinyomtatott cédulákon szereplő szavazatokat nem számolják össze, azok elsősorban a résztvevők tájékoztatására szolgálnak. Gyakorlatilag az emberek nem érezhetik magukat teljesen biztosnak abban,

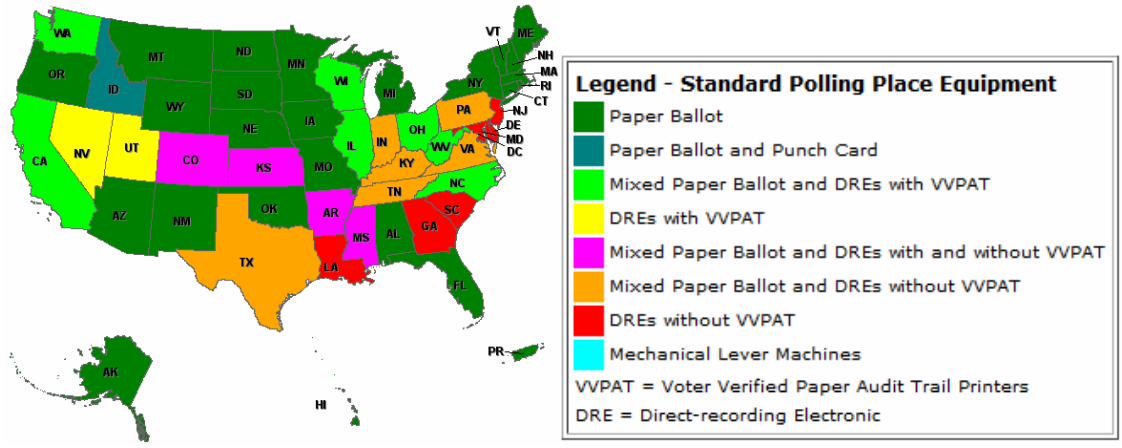
hogy a rendszerbe felvitt voksukat valóban jól számolták-e be a végeredménybe. Ezeknek a céduláknak egyébként csak akkor van jelentősége, ha újraszámlálásra kerülne sor, amely már kézi ellenőrzéssel zajlik.

Ide kapcsolódóan meg kell jegyezni, hogy 2004-ben felmerült egy olyan törvénytervezet az Egyesült Államokban, amelyben előírnák, hogy az elektronikus szavazórendszereken leadott voksoknak papíron is legyen nyoma – ezzel is erősítve a szavazók bizalmát. A papíron rögzített szavazatokat a későbbi esetleges újraszámláláskor lehetne felhasználni, és az elektronikus rendszer ezáltal ellenőrizhetőbbé válna. [6.]

A biztonsággal és privátszférával kapcsolatos további követelmények részletezése a szavazórendszerekről szóló részben találhatóak.

2.2 Az elektronikus szavazás rövid története

Elektronikus szavazási rendszereket már az 1960-as években is használtak, amikor megjelentek a lyukkártyás rendszerek. Szélesebb körben először az 1964-es elnökválasztásokkor használták őket az Egyesült Államokban, ahol hét megye választotta a lebonyolítás ezen módját. A lyukkártyás rendszerek napjainkig használatban voltak, amíg 2003-ban meg nem hozták az USA-ban azt a törvényt, amely "megszüntette a lyukkártyás szavazás addigi rendszerét és egyben kötelezővé tette a választók elektronikus nyilvántartását az Egyesült Államokban". A két rendszer pontossága közötti különbséget az a példa illusztrálja jól, hogy Georgiában 2000-ben a lyukkártyás módszerrel a szavazatok 3,5%-a volt hibás, 2002-ben (az érintőképernyős módszer használatával) viszont csupán 0,08% [7.] A csere szükségességét igazolta, hogy az Egyesült Államokban több szavazási rendszer[1] is működött az ezredfordulón (lásd: 2. ábra), amely káoszhoz és a szavazatok milliós darabszámban történő elvesztéséhez vezettek. [8.]



2. ábra: Az USA-ban használatos szavazási módszerek területek szerint [12.]

[1] Az ezredfordulón használatban levő szavazási módszerek a következők voltak: lyukkártyás rendszer, papír alapú rendszer (ahol tollal kell a szavazatot bejelölni), lézeres szkenneléssel működő rendszer, továbbá emelőkaros és elektronikus szavazógépeket is használtak a voksok begyűjtéséhez.

Az elektronikus szavazórendszerek következő változata (a lyukkártyák után) egy optikai szavazatbeolvasó rendszer (optical scan voting system) volt. Ez lehetővé tette a szavazatok automatizált beolvasását (és összeszámlálását). [3.]

A fejlődés következő lépcsőjén az ún. DRE szavazó rendszerek állnak (amelyek képesek a leadott szavazatokat összegyűjteni és csoportosítani). Ezek széles körben kerültek felhasználásra a brazíliai és indiai választásokon, valamint Venezuelában és az USA-ban is. Hollandiai pályafutásuk viszont nem volt sikeresnek mondható, igaz, hogy nagy arányban alkalmazták őket a választások lebonyolításakor, de a közvélemény aggodalmai miatt később leállították a szóban forgó rendszert.

Az internetes szavazórendszerek nagy népszerűségre tettek szert és az önkormányzati választásokhoz, népszavazásokhoz használták őket az Egyesült Királyságban, Észtországban, Svájcban és Kanadában, továbbá részben az elsődleges választásokhoz (party primary elections) az Egyesült Államokban és Franciaországban.

Az elektronikus szavazórendszerek történetében következő lépcsőként a választások lebonyolításához a mobil szavazás is szóba jöhet lehetséges megoldásként, amelynek során a résztvevők mobiltelefonjukról, az Internetről vagy digitális televíziókészülékükről is leadhatják voksukat. Azonban ez a módszer számos problémát vet fel, például a szavazók anonimitása terén (könnyen ki lehet deríteni hogy ki kit jelölt), valamint a webszerverek ellen indítható DoS (Denial of Service) jellegű támadások lehetősége is komoly problémának minősül. [7.]

Tehát elektronikus szavazórendszerre példának tekinthetők a lyukkártyákat és optikai beolvasókat használó rendszerek, a közvetlen elektronikus felvitelű szavazórendszerek (Direct Recording Electronic voting system) és a nyilvános hálózati DRE rendszerek is. Ez utóbbiak a leadott szavazatokat telefonon vagy akár az Interneten keresztül továbbítják a szavazatszámláló egységhez. A dolgozat főleg a nyilvános hálózati DRE rendszerekre fókuszál, amelyet a következő részben mutatok be.

2.3 Elektronikus szavazórendszerek

Az elektronikus szavazórendszerekkel szemben számos követelmény fogalmazódott meg az évek alatt, amelyek teljesítése elengedhetetlen a rendszer megfelelő és megbízható működéséhez. A szóban forgó követelmények az alábbiak [9.]:

- A *tökéletes titkosság* követelménye, azaz a szavazók tetszőleges részének összesített eredményét csak az összes többi szavazó összefogásával lehet megtudni.
- Az *önszámlálhatóság* követelménye: a szavazás után az összes résztvevő (illetve harmadik fél) ki tudja számítani az eredményt.
- Az *ellenőrizhetőség* követelménye: minden szavazó és kívülálló meg tud győződni arról, hogy az összes résztvevő szavazatát beleszámolták-e az eredménybe.
- Az *igazságosság* követelménye: senki sem tudhat meg semmilyen részeredményt sem a szavazás vége előtt, sem pedig utána.
- Biztosítani kell, hogy mindenki *pontosan csak egyszer szavazhat*, azaz mindenki, aki részt vett a regisztráción, legfeljebb egy szavazatot adhat le. Ha figyelembe szeretnénk venni azt, hogy valamely résztvevő meggondolhatja

magát, akkor a szavazásnál fenntarthatunk egy tartózkodott opciót is (főleg kisebb volumenű, például önkormányzati testületi ülésnél alkalmazható).

- A *jegyzőkönyvezhetőség* követelménye, azaz ha szükséges, akkor jegyzőkönyvet lehessen készíteni a szavazásról.
- A *technológiától való függetlenség* követelménye: a rendszer biztonsága ne függjön a konkrét megvalósítástól.
- A *nyílt forráskód biztosítás*ának követelménye, azaz a rendszer biztonsága ne függjön az algoritmus vagy a program forráskódjának titkosságától.
- Az *ellenőrizhető szavazógép* követelménye: minden egyes résztvevő leellenőrizhesse a szavazógépet a szavazás előtt.

2.3.1 Nyilvános hálózati DRE rendszerek

[5.] Választásokat teljes egészében csupán DRE szavazórendszerekre (Direct Recording Electronic voting systems) alapozva először 1996-ban Brazíliában bonyolítottak le. 2004-ben az Egyesült Államok regisztrált szavazóinak körülbelül harmada használt DRE rendszert a szavazásokkor. Ezekből az adatokból is látszik a szóban forgó rendszerek növekvő elterjedése.

3. ábra: Egy Brazíliában használatos szavazógép

A nyilvános hálózati DRE szavazórendszer egy olyan elektronikus rendszer, amely elektronikus szavazólapokat használ és továbbítja a nyilvános hálózaton keresztül a szavazati adatokat a szavazó helyről egy másik helyre (ahol majd a számlálás megtörténik).

A szavazásra vonatkozó adatok többféle módon gyűjthetőek össze. Egyik módszer az, amikor egyesével továbbítják a szavazatokat, pont úgy, ahogy azok generálódnak a szavazóhelyeken. Másik megközelítés szerint megvárják, amíg egy bizonyos mennyiségű szavazat összegyűlik és kötegekben/csomagokban továbbítják őket (a választások teljes időtartama alatt, napjában akár többször is). A harmadik módszer szerint megvárják, amíg az összes szavazat beérkezik, majd a választás legvégén, egyetlen kötegben továbbítják a szavazás adatait az arra kijelölt helyre.

Nyilvános hálózati DRE rendszernek tekinthetőek azok a rendszerek is, amelyeknél az *Interneten keresztül* történik a szavazás lebonyolítása. Egyik ilyenre mutatott példát[2] Svájc, ahol 2004 szeptemberében elsőként próbálták ki az Internet- illetve e-mail alapú elektronikus szavazási rendszert. "Genf kanton néhány városában beváltotta a hozzá fűzött reményeket: biztonsági problémák nem merültek fel, és valamelyest a szavazókedvet is élénkítette a nappaliból elérhető virtuális szavazóurna." Az érintett településeken átlagosan minden ötödik szavazópolgár Interneten keresztül adta le a voksát. Ehhez a lehetőséghez a svájci választók egy kártyát kapnak az önkormányzattól, amely egy 16 számjegyű kódot, és egy négy karakteres biztonsági kódot tartalmazott. A szavazás az önkormányzat választási weboldalán történt, a személyi kód, a biztonsági kód és a személyes adatok megadása után. A 2004 szeptemberében megtartott népszavazáson "a genfiek 72,5 %-a postai úton, 22 %-a az Interneten keresztül ikszelt, és mindössze 5,7 %-uk ment el a szavazófülkébe." [10.]

Az internetes szavazást egyébként gyakran használják a vállalatok és szervezetek hivatalnokaik (officers) és az igazgatósági tagok (board members) megválasztására is.

2.3.1.1 Egy egyszerű példa

Egy nagyon egyszerű, szavazást lebonyolító rendszerre példa lehet az alábbi.

Tegyük fel, hogy a modellben csak két résztvevő van: a választópolgárok és a választási szerver, amelyet a választásokat lebonyolító hatóság üzemeltet. Ennek a hatóságnak a feladata ellenőrizni a polgárok részvételi jogosultságát, továbbá összegyűjteni és összeszámolni a szavazatokat. A példához egy olyan előfeltételezés szükséges, hogy a választópolgárok be legyenek regisztrálva a választási szervezetnél a szavazás megkezdése előtt.

Az egyszerű példa működési protokollja az alábbi:

- A szavazó elküldi a szavazatát a szavazó azonosítójával (voter ID) együtt a szervernek.
- A szerver a szavazó azonosítóját használja annak ellenőrzésére, hogy a szavazó regisztrálva van-e és szavazott-e már.
- Ha a szavazó regisztrálva van és jogosult szavazni, akkor a szerver feljegyzi a szavazatot és hozzáadja a választási összesítőhöz.

Egy ilyen egyszerű protokoll működésével kapcsolatban is merülhetnek fel problémák. Például a szavazók megszemélyesíthetőek (a szavazatok bármilyen érvényes szavazói azonosító alatt elküldhetőek), ez *hitelesítési* gondokat jelent. Ha a szerver nem működik megfelelően, akkor módosíthatja a voksot, esetleg ő maga is összeállíthat és elküldhet érvényes szavazatot (amelynek következtében a jogosult személyek elesnek a szavazás lehetőségétől, mert az azonosítójukat a szavazógép már felhasználta egy voks generálásához). Ez a fajta támadási lehetőség *integritási* problémákat vet fel. A szavazók ezeken felül nem tudják ellenőrizni, hogy a szavazatuk helyesen lett-e tárolva, amely az *ellenőrizhetőség*i követelményhez kötődik. És végül (ami minket leginkább

[2] Az adott évben megtartott svájci népszavazás kérdésköre nem bírt akkora politikai fontossággal mint egy elnökválasztás: a résztvevők arról dönthettek, hogy az adófizetők pénzéből finanszírozzák-e egy étterem felújítását. Ez a népszavazás tökéletes próbát biztosított az Interneten lebonyolítható szavazási módszer számára.

érdekel) a *privacy*-vel kapcsolatos probléma: a szerver látja, hogy ki kire/mire adta le a szavazatát (a szavazói azonosító alapján).

Az egyszerű példához kötődően a korábbiakban ismertetett, elektronikus szavazórendszerekkel szemben támasztott követelmények (főként biztonság és privacy tekintetében) az alábbiakkal bővíthetőek ki:

- Fontos annak biztosítása, hogy *csak a jogosult szavazók* szavazhassanak (egyénenként egyszer, ahogy az korábban meg lett említve).
- A szavazókat *ne lehessen megszemélyesíteni*. (Tehát rossz indulatú személyek ne tudják becsapni a rendszert és ne tudják másnak kiadni magukat, más nevében szavazni.)
- Ha a szavazatokat egyszer már leadták, ne lehessen azokat *utólag módosítani*, *kivenni* az összeszámoltak közül (ezzel is módosítva a szavazás kimenetelét), továbbá nem lehet *érvénytelen* szavazatot beszámítani a végső összesítésbe.
- Sem a választási hatóságok (sem pedig más) ne tudja *összekapcsolni* a szavazatokat az azokat leadó választókkal.
- Egy másik érdekes követelmény, hogy a szavazók *ne tudják bizonyítani*, hogy kire szavaztak, máskülönben a szavazataik eladhatóak lennének.

2.3.1.2 DRE szavazórendszerek

A DRE szavazórendszerek esetén a hagyományos, papír alapú választási megoldásokhoz hasonlóan a résztvevők ellátogatnak a szavazókörzetükbe, hogy voksaikat leadják. A DRE rendszereknél azonban a szavazáshoz nincs szükségük papírra és tollra.

A DRE rendszerek általános működése:

- A szavazás első lépéseként a résztvevők igazolják, hogy jogosultak szavazni, ehhez esetleg szükségük lehet egy személyigazolványra.
- Második lépésként a szavazó felmutat egy tokent[3] a rendszer számára, majd leadja voksát a kiválasztott jelöltre.
- Amikor a résztvevő végzett a jelöléssel, akkor a DRE rendszerek többsége lehetőséget biztosít számára, hogy áttekintse leadott szavazatait (és ha szükséges, még módosítson rajta ha elrontotta).
- Ezt követően a szavazat leadásra kerül és a szavazó nyugodtan távozhat.
- A leadott szavazatokat elmentik és memória modulokon továbbítják egy központi helyre, szavazatszámlálási célból.

A DRE rendszerek kiegészíthetőek VVPAT (Voter Verifiable Paper Audit Trail) lehetőséggel úgy, hogy egy nyomtatót csatlakoztatnak a rendszerhez. A VVPAT-ról a bevezető részben már tettem említést.

---

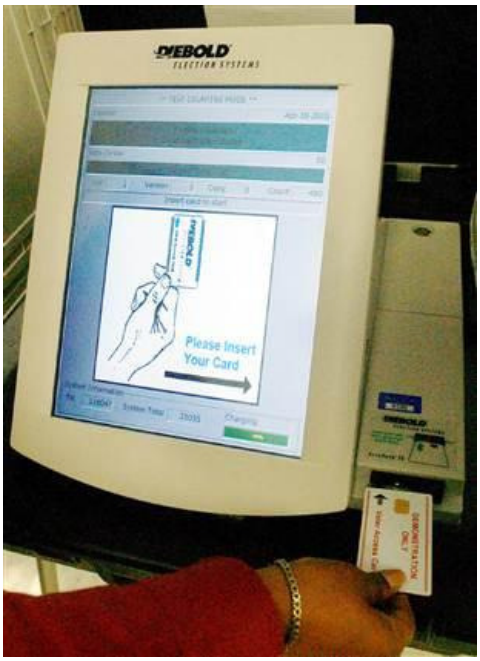
[3] Token alatt érthetünk PIN kódot, smart kártyát vagy bármi olyan eszközt, amely lehetővé teszi a felhasználó számára, hogy hozzáférjen a szavazóterminálhoz.

A DRE rendszerekkel adódtak problémák. Gondot jelenthet, hogy az egész választás kimenetele a terminál korrektségén/megbízhatóságán, robosztusságán és a benne levő hardver és szoftver biztonságán alapul. Ha a kód tele van biztonsággal kapcsolatos problémákkal, akkor ezek a hibák könnyen kijátszhatóak mind a rosszindulatú szavazók, mind a rosszindulatú bennfentesek által (pl. a tisztviselők akik felügyelik a választási folyamatot, a szavazórendszer fejlesztői illetve annak a beágyazott operációs rendszernek a fejlesztői, amelyen a szavazó rendszer fut).

A DRE rendszerek biztonsági problémáira egy hírhedt példa a Diebold szavaztató gépe, amelyről a következőkben fog szó esni.

2.3.1.3 A Diebold szavazórendszer és problémái

[11.] Szavazások lebonyolításához számos gyártó kínál eszközöket, többek között a Diebold, Hart InterCivic, Sequoia, AccuPoll, Avante és sokan mások. A használatban levő különböző eszközöket évekkel ezelőtt vizsgálatoknak vetették alá az Egyesült Államokban, mielőtt az előző választások elkezdődtek volna. A Diebold, Hart InterCivic és a Sequoia gyártmányait (biztonság tekintetében) nem találták megfelelőnek és így leminősítették a vizsgáló szervezetek. A feltárt problémák orvoslására az ún. Open Voting rendszert kívánták bevezetni, amely a szavazás végén kinyomtat egy űrlapot, amit a résztvevő maga tud ellenőrizni (erről majd az Open Voting Consortium-ról szóló részben részletesebben esik szó).



4. ábra: A Diebold egy szavazókészüléke

A Diebold szavazó berendezésével kapcsolatban számos tanulmány született, amelyek a biztonságosságát voltak hivatottak feltárni. Ezek közül egy a [14.]-es irodalomban található. A rendszer gyengeségei közül azokat említeném meg, amelyek főként a szavazók privacy-jével kapcsolatosan kritikusak.

A Diebold rendszerrel a választás menete a következő módon zajlik:

- Egy szavazókártyát (ami lehet egyaránt memóriakártya vagy smart kártya) adnak minden választónak a szavazást lebonyolító helyen.
- A szavazó beilleszti a szavazókártyáját a terminálhoz kapcsolt kártyaolvasóba.
- A terminál ellenőrzi, hogy az olvasójában levő kártya egy szavazó kártya-e. Ha igen, akkor egy szavazó űrlapot jelenít meg a terminál kijelzőjén.
- A szavazó úgy lép interakcióba a terminállal, hogy a megfelelő négyzeteket megérinti a kijelzőn. (Fejhallgató és billentyűzet áll a látássérült szavazók rendelkezésére, hogy titkosan (privately) léphessenek kapcsolatba a terminállal.)
- A szavazónak végül lehetőséget adnak, hogy ellenőrizze választásait mielőtt az rögzítésre kerülne.
- Ha a választó megerősíti a visszajelzett szavazatait, akkor azokat feljegyzi a terminál és a szavazó kártyát érvényteleníti (azért, hogy egy azon szavazó ne adhasson le több szavazatot).
- A szavazó ezt követően visszaviszi az érvénytelenített kártyát a szavazási biztosoknak, akik újraprogramozzák (ismét érvényessé teszik) a következő választó számára.

A rendszer számos gyengeséggel rendelkezik, főként a biztonság terén. Egy támadó számára lehetőséget biztosít a szavazás tönkretételére (működésképtelenné tudja tenni a terminált), többszörös szavazatok leadására (amennyiben a támadó előre olyan szavazókártyát készített házilag, amely figyelmen kívül hagyja az érvénytelenítési műveletet), le tud adni hamis szavazatokat, meg tudja akadályozni a választási adatok redundáns tárolását stb.

A Diebold rendszer kifogásolható technikai megoldásai közé tartozik többek között az, hogy a leadott szavazatokat generálási sorrendben írják be a tárolásukra szánt fájlba. Így ha a szavazást felügyelő bizottsági tagok közül egyvalaki feljegyzi, hogy az adott terminálokon kik és milyen sorrendben szavaztak, akkor a választópolgárokat össze tudják később rendelni a szavazataikkal.

Egy későbbi cikk kapcsán kiderült, hogy a Diebold rendszerében tárolt szavazatokhoz időbélyeg is hozzárendelésre kerül. Ha valaki tehát rendelkezik a szavazók érkezési sorrendjét (a helyszínen történő bejelentkezési idejét) tartalmazó dokumentumokkal, akkor az elektronikusan tárolt információk és a szóban forgó dokumentum alapján könnyen össze tudja rendelni, hogy ki kire voksolt. Privacy tekintetében ez egy komoly probléma. [18.]

2.3.2 Tanulságok, következtetések

Általánosságban elmondható, hogy a DRE rendszerek tervezésénél figyelni kell tehát arra is, hogy a rögzítésre kerülő szavazatok ne tartalmazzanak például időbélyegeket. Ez azért lehet problémás, mert ha a szavazókörzetbe érkezőket egy rejtett kamerával sorra vesszük, majd a választás végén a gépeken eltárolt voksok időbélyegeit elemezzük, könnyedén össze tudjuk rendelni a polgárokat a választásukkal. [17.] Az időbélyegekkel kapcsolatos másik felmerülő probléma a VVPAT-ot használó rendszereknél került elő. Ott ugyanis a kinyomtatott űrlapokon bizony megtalálható a szavazás pontos időpontja (amely bárki számára hozzáférhető), így ennek ismeretében a szavazók és szavazataik

összerendelése ismételten nem jelent túl nagy kihívást. A Diebold-nál azért arra figyeltek, hogy a VVPAT-tal kiegészített rendszerük ne nyomtassa ki a szavazás időpontját, de a rögzített állományok esetében ez a mozzanat kimarad (ahogy korábban említettem).

Az elektronikus szavazórendszereknél a résztvevők anonimitása erősen függ a szavazataikkal való összeköthetetlenségtől illetve a résztvevők titkosságától. Ha elektronikus szavazásra kerül a sor, gyakorlatilag egy erős falat kell tudnia építeni a rendszer megalkotóinak a szavazatok és az azokat leadó személyek közé (azért, hogy az *összerendelhetetlenséget* biztosítsák). Tehát ha ismerünk egy szavazatot, akkor nem tudhatjuk, hogy ki adta le, illetve ha tudjuk hogy valaki részt vett a szavazáson, akkor ne tudhassuk, hogy kire adta le a voksát. Erre a problémára már próbáltak matematikai megoldásokat hozni, az egyik amire említést találtam az a Multi-Party (MP) protokoll. [19.] A megjelölt oldalon több olvasmány is található ezzel kapcsolatban, illetve a szóban forgó protokoll biztonságát bemutató dokumentum is [20.].

Tanulságként levonhatjuk azt, hogy ezen rendszerek fejlesztésénél még nem léteztek egységes szabályok, szabványok, amelyeknek a gyártóknak meg kellett volna felelniük. Gondot jelentett az is, hogy az egyes vállalatok a saját rendszereiket elzártan, kíváncsi tekintetektől védve fejlesztették (és így rejtve maradtak a készítők előtt olyan problémák, amelyek a biztonsággal és privacy-vel kapcsolatos aggodalmaknak adhatnak okot). Ha nem így tettek volna, akkor különböző szervezetek, kutatók, szakemberek segíthettek volna nekik a kritikus hibák felfedésében. Szerte a világon, ezeket a tényeket felismerve próbálják a jövő szavazórendszereit sokkal biztonságosabbnak (egységesebbnek, szabványoknak megfelelőnek) elkészíteni, méghozzá egy bárki által figyelemmel kísérhető folyamat során.

2.4 Open Voting Consortium

[13.][15.][16.] A nyílt szavazórendszerek fejlesztésének támogatásával az OVC (Open Voting Consortium), egy non-profit szervezet foglalkozik. Nemzeti és nemzetközi szabványok megalkotásában egyaránt részt vesznek. Céljuknak tűzték ki az univerzális szavazógépek megteremtését, amelyekre az elmúlt években fellépő -és egyre növekvő- igény mutatkozik. (A közelmúltban lezajlott, főként amerikai választások problémáinak egy részét a felszerelés sokfélesége és nem-megfelelősége okozta. Ezeket a gondokat szabványok segítségével orvosolni lehet.)

Elképzeléseiknek megfelelően elkészítették a saját szavazógépüket, amelynek fő jellemzői a következők:

- Egy átlagos PC-n kiválóan üzemel, de szükséges hozzá érintőképernyő.
- CD-ről bootol, nincs szükség merevlemez meglétére.
- A rendszer működéséhez szükség van továbbá egy (a géphez kötött) nyomtatóra.
- A rendszer a szavazásról előállít egy űrlapot, amely egyrészt az emberek számára olvasható szöveges információt, továbbá egy vonalkódot tartalmaz.
- A kinyomtatott űrlapot egy gyűjtőládában kell elhelyezni a szavazás megtörténte után. (Máskülönben a szavazásról készült visszaigazoló lappal bizonyítható lenne hogy ki kire szavazott, és a szavazatok megvásárolhatóak lennének.)
- A szavazatok összeszámlálásához a vonalkódokat olvassák be.

Az általuk kidolgozott rendszer teljesíti többek között azt a követelményt, hogy a választási biztosok nem tudják meghatározni, hogy a szavazók kire adták le a voksukat. A megtervezésnél az egyik legfontosabb cél az volt, hogy az elkészített gép egy egyértelmű/félreérthetetlen papírt nyomtasson a leadott szavazatról, ráadásul az összes fajta szavazólap ugyanúgy nézzen ki (függetlenül attól, hogy ki nyomtatta azt ki – például látássérültek számára összeállított szavazóhelyen nyomtatták ki vagy egy átlagos szavazóhelyen). Erre a követelményre azért van szükség, hogy a szavazók és leadott voksaik ne legyenek összerendelhetőek az esetleges plusz információ alapján (pl. ha egy szavazókörzetbe csak egy látássérült ment szavazni és csak ő szavazott az adott speciális terminálon).

Ennél a rendszernél a vonalkódot úgy tervezték meg, hogy a szükséges azonosítókon kívül (pl. dátum, választás, körzet, szavazóterminál, véletlen szavazólap-azonosító) tartalmazza a polgár választását, egy ellenőrző összeget, továbbá kiegészítő adatokat a választási biztosok számára (akik a nyomtatott szöveges részt nem látják, csak a vonalkódokkal kerülnek kapcsolatba, így nem tudják meg hogy a résztvevő kire voksolt), de mégse lehessen a választók személyét megtudni a nyomtatott lapon található információk alapján. [17.]

Nem csak az OVC, de más szervezetek, kutatók is fáradhatatlanul keresik azokat a technikai megoldásokat, amelyek lehetővé teszik a régi papír alapú választási rendszerek lecserélését számítógép alapú szavazási rendszerekre. Ezen a téren aktív kutatások zajlanak, egyre nagyobb figyelmet fordítanak a választók anonimitásának kérdésére is. A témával kapcsolatos további cikkek (amelyek az utánuk jelölt hivatkozott linkeken találhatóak):

- Robert Krimmer, Melanie Volkamer, "Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting." EGOV06 Conference, Krakow, Poland, 2006 [21.]

- Yi Mu, Vijay Varadharajan, "Anonymous Secure E-Voting over a Network" [22.]

- Sean Peisert, Matt Bishop, Alec Yasinsac, "Vote Selling, Voter Anonymity and Forensic Logging of Electric Voting Machines" [23.]

3 Összefoglalás

A népesség megfelelő részét érintő, fontos kérdésekben szavazásra van szükség a döntések meghozásához. Ezen folyamat lebonyolítására manapság számos mód kínálkozik (a papír alapú megoldásoktól az elektronikus lehetőségekig bezárólag).

A módszer kiválasztásában nagy szerephez jut a kérdés fontossága. Ez azt befolyásolja, hogy a hibák mennyire megengedhetőek a szavazás lebonyolítása során, mennyire megbízható megoldást kell választani, mekkora a megengedett költség a szavazás során stb. Tehát ha egy kevésbé fontos kérdésben kell a szavazók véleményét kikérni, akkor megelégedhetünk egy olcsóbb, kis mértékű hibát produkáló, egyszerű rendszerrel is. Azonban ha nagyon fontos kérdésben kell dönteni (például egy elnökválasztás során), akkor természetesen a megbízhatóság és a biztonság elsődleges szempont, ilyenkor a pénz kevésbé számít.

A módszer kiválasztásánál azt is figyelembe kell venni, hogy az emberek hány százaléka számára érhető el az a technika, amelyet használni kívánunk. Például nem biztos, hogy az Interneten keresztül lebonyolított szavazás számít jó megoldásnak egy olyan kérdés esetén, ahol mondjuk az idősebb korosztály véleményét is ki akarjuk kérni (hiszen sok nyugdíjas nem rendelkezik világhálóra kötött számítógéppel). Vagy másik ilyen példa az SMS, amelynek megírásával tipikusan az öregebb korosztálynak vannak gondjai.

A jövőben várhatóan az elektronikus szavazási módszerek leváltják a hagyományos szavazási módszereket, amennyiben a technológia (és annak könnyű hozzáférhetősége bármelyik szavazó ember számára) ezt lehetővé teszi. A jelenleg meglévő módszerek problémáit, hiányosságait mind a biztonság, ellenőrizhetőség és privacy területén igyekeznek kiküszöbölni, megszüntetni.

A dolgozatban bemutatásra kerültek az elektronikus szavazórendszerekkel kapcsolatos követelmények, ezen rendszerek gyakorlatban megvalósult szereplései, eredményei, valamint a rendszer sérülékenységét, problémáit bemutató Diebold esettanulmány, amelynél láthattuk, hogy számos továbbfejlesztési lépés szükséges ahhoz, hogy a jövőben tényleg megbízható, a választók anonimitását garantáló rendszerek képezzék a szavazások alapját.

Irodalomjegyzék

[1.] http://www.torilecke.com/fenykepek/2-okor/okor---gorog-varosallamok/16.-osztrakon-themisztoklesz-nevevel.html, 2012.05.03. 18:07

[2.] http://en.wikipedia.org/wiki/Electronic_voting, 2012.05.03. 19:19

[3.] http://en.wikipedia.org/wiki/Optical_scan_voting_system, 2012.05.03. 20:38

[4.] http://www.electronic-vote.org/TERMINI/vvpat_en.php, 2012.05.03. 21:13

[5.] http://en.wikipedia.org/wiki/DRE_voting_machine, 2012.05.03. 20:53

[6.] http://pcworld.hu/papiron-dokumentalt-elektronikus-szavazas-20040429.html, 2012.05.04. 13:17

[7.] http://www.netlock.hu/html/sajtofigyeles/nonpublic/archiv/news/05/0547.html, 2012.05.04. 13:24

[8.] http://www.origo.hu/nagyvilag/20010727hatmillio.html, 2012.05.04. 13:46

[9.] http://www.rfid.answare.hu:8080/site/kutatasi-erdmenyeink/biztonsagi-megoldasok/2007/szabadalmi-bejelenteseink/szavazatszamlalo_rendszer-szabadalmi_beadvany.doc/view, 2012.05.04. 14:33

[10.] http://www.hullamvadasz.hu/index.php3?tanulmany=632.&fejezet=3&szabadpolc=1, 2012.05.04. 18:52

[11.] http://wildbee.org/2008/10/17/open-source-voting-transparent-cheap-and-you-get-to-read-your-ballot/#more-24, 2012.05.04. 20:54

[12.] http://verifiedvoting.org/verifier/index.php?ec=standard&state=&year=2010, 2012.05.04. 21:59

[13.] www.nist.gov/itl/vote/upload/Abercrombie.pptx, 2012.05.04. 22:09

[14.] http://static.usenix.org/event/evt07/tech/full_papers/feldman/feldman_html/, 2012.05.04. 23:44

[15.] http://wildbee.org/2008/10/17/open-source-voting-transparent-cheap-and-you-get-to-read-your-ballot/, 2012.05.04. 23:52

[16.] http://www.openvotingconsortium.org/, 2012.05.05. 00:27

[17.] http://gnosis.cx/publish/voting/electronic-voting-machine.pdf, 2012.05.05. 12:16

[18.] http://www.techdirt.com/articles/20070820/113332.shtml, 2012.05.05. 14:09

[19.] http://safevote.com/election.htm, 2012.05.05. 14:29

[20.] http://safevote.com/doc/thebell1.8.pdf, 2012.05.05. 14:32

[21.] https://docs.google.com/viewer?a=v&q=cache:2Na5psDh6wsJ:www.e-voting.cc/files/Working-Paper-1-2006/+&hl=hu&gl=hu&pid=bl&srcid=ADGEESi33-diP_Ejq2ILYebFuFfQXWTYpGEr1Yh4QIu8l1lHxPMhqmr-hKHCN4VW-u2mfCkoVHtsBo3NscqDZ2qkJFsTibYFing5Dyz4xFuB4ci_44OYZ12SuKM8rZ8Ilrd9URy8xEQg&sig=AHIEtbRIuYrNcBxowgzOQtFZEDc6jg9dFQ&pli=1, 2012.05.05. 15:19

[22.] http://www.google.hu/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CHkQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.25.8881%26rep%3Drep1%26type%3Dpdf&ei=ximlT6aCOsHZtAbryIH8BA&usg=AFQjCNHEmCogsbAP_D_EsJtPkbUZnsCf3Q&sig2=Kho2CIIyqSMN2Xf29NK0PA, 2012.05.05. 15:24

[23.] http://nob.cs.ucdavis.edu/bishop/papers/2009-hicss-2/votelog.pdf, 2012.05.05. 15:28

Ábrajegyzék