Kara Péter András

Tradicionális szavazórendszerek privacy kérdései, elemzésük és bemutatásuk PET-szerűen

20. téma

Tartalomjegyzék

1 Bevezető

A modernkori demokrácia egyik alappillére a többség akaratának érvényesülése. Ezen gondolat gyakorlati kivitelezése az ókori görög világból ered, nevezetesen az athéni demokrácia által implementált híres-neves cserépszavazás nevezetű eljárásból. Alapvető funkciója a különböző okok miatt nemkívánatos személyek eltávolítása volt, mely megakadályozta zsarnoki beállítottságú vezetők uralmát, csökkentette a népben felgyülemlő feszültséget és megelőzte az esetleges komolyabb belső ellentétek eldurvulását.

Ahogy a mai világban is, a szavazójog egy állampolgári jog, egy véleménynyilvánítási lehetőség, nem pedig kötelesség, bármennyire is sokakban él ma eme tévhit. Az ókori athéniakra is érvényes volt ez; az szavazott, aki rendelkezett szavazati joggal s élni is óhajtott szavazati jogával. Ennek függvényében világos volt, hogy különböző szavazások különböző részvételi aránnyal rendelkeznek. Emiatt a szavazás érvényességéhez meghúzásra került egy minimális részvételi létszám, mely akkoriban nem százalékban, hanem darabszámban lett meghatározva, konkrétan legalább 6000 szavazatra volt szükség.

Mint ahogy az már említve lett, a szavazások célja a társadalom harmóniájára veszélyt jelentő egyének eltávolítása volt. Eltávolítás alatt száműzetésre kell gondolni, mégpedig egy tíz éves időtartamra. A szavazóképes polgárok azon egyén nevére szavaztak, kit átmeneti száműzetésbe óhajtottak taszítani; aki a legtöbb szavazatot kapta, annak kellett távoznia.

Maga az eljárás nevét egy rendkívül ötletes költséghatékony megoldásból kapta. Míg manapság a tradicionális parlamenti választások és népszavazások során egészen megrendítő pénzösszegek kerülnek elköltésre a procedúra lebonyolítására, addig az ókori athéniak ezt hulladék-újrafelhasználással kombinálva törött cserépdarabokkal végezték. A szavazók a „jelölt” nevével ellátott cserépdarabokat helyezték el szavazatgyűjtési urnákba, melyek az érvényességi számot elérve csoportosításra, megszámlálásra kerültek.

Vajon kifogástalan volt eme rendszer privátszféra technológia tekintetében? Elsőnek is vizsgáljuk meg a dolgot a tradicionális és elektronikus szavazórendszerekkel szemben támasztott alapkövetelmények szempontjából.

1. ábra: Cserépdarab Periklész ellen. A cserépdarabon feltüntetve apjának a neve is, egyértelműsítési célokból, mint ma egy személy anyjának leánykori neve.

- *Mindenki szavazhat, aki szavazásra jogosult, de más nem.* E feltétel teljesülésének nincs elméleti gátja.

- *Minden szavazásra jogosult polgár egyszer szavazhat.* Ez már kevésbé triviális teljesen hibamentes teljesülés tekintetében, hisz egy tízezres nagyságrendű szavazószám mellett központi szavazói adatbázis hiányában előfordulhat, hogy egy kevesek által ismert, átlagos kinézetű polgár akár kétszer adjon le szavazatot. Sőt, akár kivitelezhető szavazórendszer elleni támadás, ha az adott polgár a cserépdarabot egy nagyjából felénél lévő vonal mentén kettétöri, a cserép egyik oldalán a vonaltól balra, másik oldalán pedig a vonaltól jobbra írja fel a jelölt nevét s a két darabot összeillesztve szavaz, mely a szavazás pillanatában szavazóhatósági szemszögből egy szavazatnak tűnhet, míg valójában a szavazatszámlálás során két külön szavazatként lesz számolva.

- *Minden érvényes szavazatot kötelező pontosan egyszer számításba venni, s utólag kiegészített, csalárd szavazatokkal nem befolyásolható az eredmény.* Itt is megkérdőjelezhető a rendszer, hisz elég arra gondolni, hogy a szavazási eszköz a szavazat leadása és annak megszámlálása között megsérülhet, egy törött cserépdarabról lévén szó. Arról nem is beszélve, hogy a száműzetésre jelölt egyének neve akár kis differenciájú is lehet, melyek garantált megkülönböztetését nehezítheti azon tény, miszerint a választópolgár maga írja le a nevet, s ahogy az a fennmaradt darabokon is látható, gyakran fel sem tüntették a célszemély apjának nevét, mely segítene a megkülönböztetésben. Tízezres nagyságrendű szavazatszámlálás matematikai és erkölcsi korrektsége még külön kérdéseket vethet fel.

További alapfeltételi szempontok szerint is lehetne elemezni a választási rendszer helyességét, számunka azonban nem a hagyományos értelemben vett választási csalási formák vagy inkorrektségek az érdekesek, hanem a szavazási privátszféra

sérthetetlensége. PET technológiailag indifferens, hogy egy szavazás során az összeszámlált eredmény nem felel meg pontosan a szavazók akaratának, véleményének.

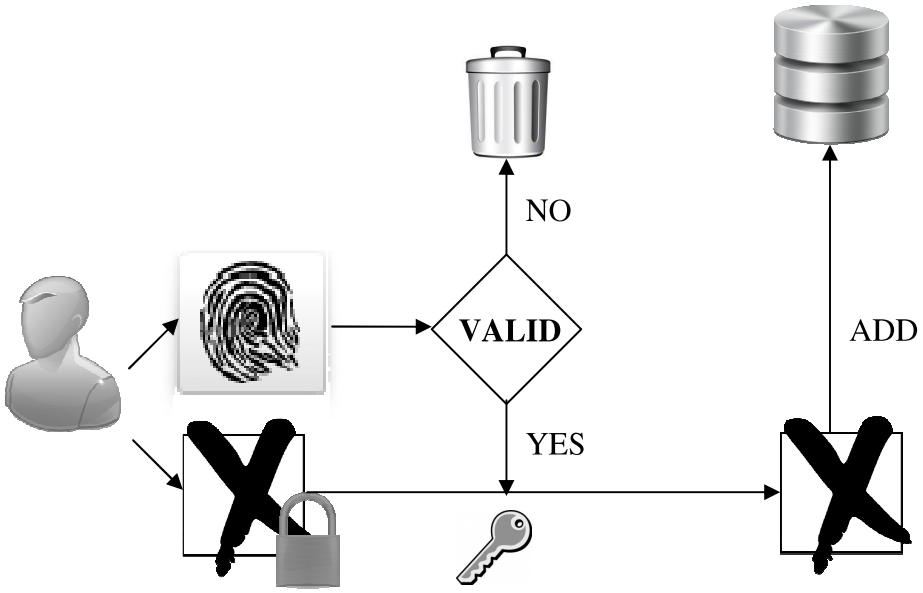
Ami fontos, hogy névtelen szavazásról lévén szó, a szavazat ne legyen összepárosítható a szavazóval. Ilyen információ a szavazópolgárral szemben rendkívül súlyos negatív megkülönböztetést eredményezhet, anyagi és egészségügyi károkat okozhat. Manapság is egy teljesen egyértelműen kezelt dolog, hogy egy névtelen szavazáskor, például parlamentáris választáskor, a szavazó által leadott szavazat kizárólag a szavazóra tartozik, senki más nem jogosult eme információ megismerésére. Ugyanúgy, ahogy teljességgel erkölcstelen és elfogadhatatlan, hogy egy munkáltató az állásinterjú során érdeklődjön a munkára jelentkező politikai szimpátiájáról, hovatartozásáról. Az ókori Athénban zajló szavazásokon esetlegesen előforduló szavazat/szavazó párosításnak természetesen foglalkozásbeli vagy egzisztenciális következményeknél súlyosabb kihatásokkal is járhatott, elég arra a példára gondolni, hogy így akár egy politikailag befolyásos személy pontos listát kaphatott azon személyekről, kik ellene szavaztak, melyet saját kreatív eszközvilágával megtorolhatott.

PET tekintetében az ókori athéni cserépszavazás egy naiv tradicionális szavazórendszer implementáció. Elsőnek is nem volt központilag elfogadott, kellően védett szavazatadási hely. Semmi nem garantálta, hogy a cserépdarab szavazattal történő ellátása és az urnába helyezés ideje között más ne juthasson vizuális úton a szavazati információhoz. Kézírással történő szavazásról lévén szó a grafológiai információszivárgás lehetősége is adott volt. Ezen felül maga a szavazóobjektum is szavazói személyes információt képes hordozni azáltal, hogy az adott formájú, színű, mintázatú, jellegzetes ismertetőjegyű cserépdarab alapján akár beazonosítható a szavazó, így összepárosítván a szavazatot a szavazóval.

2. ábra: Hipparchus nevét hordozó cserépdarab. Amennyiben ezen cserépdíszítési minta kizárólag az adott szavazó által volt használva, személye könnyen hozzárendelhető volt szavazatához.

2 Anonim szavazórendszerek privátszférája

Ahogy az a bevezetőben is ki lett emelve, tradicionális anonim szavazórendszereknél az egyetlen igazán fontos privacy kérdés a szavazó és a szavazat összeköthetősége (linkability). Ennek szükséges feltétele, hogy a szavazás teljes életciklusa során ne jöhessen létre olyan rögzített adat, mely vagy az adott szavazóhoz hozzárendel egy szavazatot vagy pedig a lehetséges döntések halmazát szűkíti, esetleg eltérő valószínűségeket rendel a szavazati lehetőségekhez. Abban az esetben, ha létrejönne a procedúra során egy egyértelmű szavazat/szavazó párosítás, alapvetően megkérdőjelezné a teljes anonimitás teljesülésének lehetőségét.



3. ábra: Teoretikus szavazórendszer. Érvénytelen vagy már használt azonosító esetén a teljes szavazómédium megsemmisítésre kerül. Sikeres hitelesítés esetén a szavazat már az azonosító nélkül megy tovább a rendszerben, ahol dekódolásra majd feldolgozásra kerül.

Példa erre egy olyan elképzelt, tradicionális szavazórendszer, ahol az authentikáció a szavazatra, nem pedig a szavazóra vonatkozik. A szavazó feltünteti egyedi azonosítóját a szavazati médiumon, mely a szavazatok összeszámlálásakor kerül hitelesítésre. Természetes elképzelhető olyan megoldás, mely emberi szavazatösszesítés során is meg próbálja őrizni a felhasználó anonimitását. Ilyen implementációs lehetőség, ha a hitelesítés után a szavazat és a hitelesítési felület szeparálásra kerül, például perforálás útján.

Az elsődleges probléma ezzel az, hogy a szavazói anonimitás ki van téve a rendszer esetleges meghibásodásának veszélyének. Mivel a szavazó személyi fedőnevet használ, kiléte nyílt. Hiteles összeköthetőséget biztosító, egyedi szerepazonosító esetén továbbra is garantálható, hogy csak az szavazhasson, aki jogosult rá, s adott szavazó részéről csak egy szavazatot lehessen érvényesen számításba venni. Ennél biztonságosabb implementáció, ha a szavazó a szavazás előtt közvetlenül egy tranzakciós azonosítót kap, mely egyszer használatos s élettartalma minimális, ez azonban értelmetlenné tenné az egész rendszert, hisz a tranzakciós azonosító kiadásához a szavazó hitelesítésére lenne szükség. Egy másik probléma még, hogy a szavazó nem tudja követni az életciklus során az érzékeny adatok sorsát.

Környezettől és céltól függően, egy szavazás természetesen lehet kötelező jellegű is, például titkos szavazás egy cégnél, ahol egy adott csoport minden tagjának döntést kell hoznia. Amennyiben önkéntes szavazásról beszélünk, privát információ lehet például akár a szavazás ténye is. Ilyenkor szükséges az észlelhetetlenség kritérium teljesülése, a szavazatok szteganográfiai védelme.

Miért lehet védendő információ a szavazás ténye? Mitől számíthat az problémának, ha az adott szavazóról tudni lehet, hogy hivatalosan véleményt nyilvánított-e egy ügyben, avagy nem? Nem nehéz olyan példát mutatni, ahol a szavazás tényének védelme a szavazó érdeke.

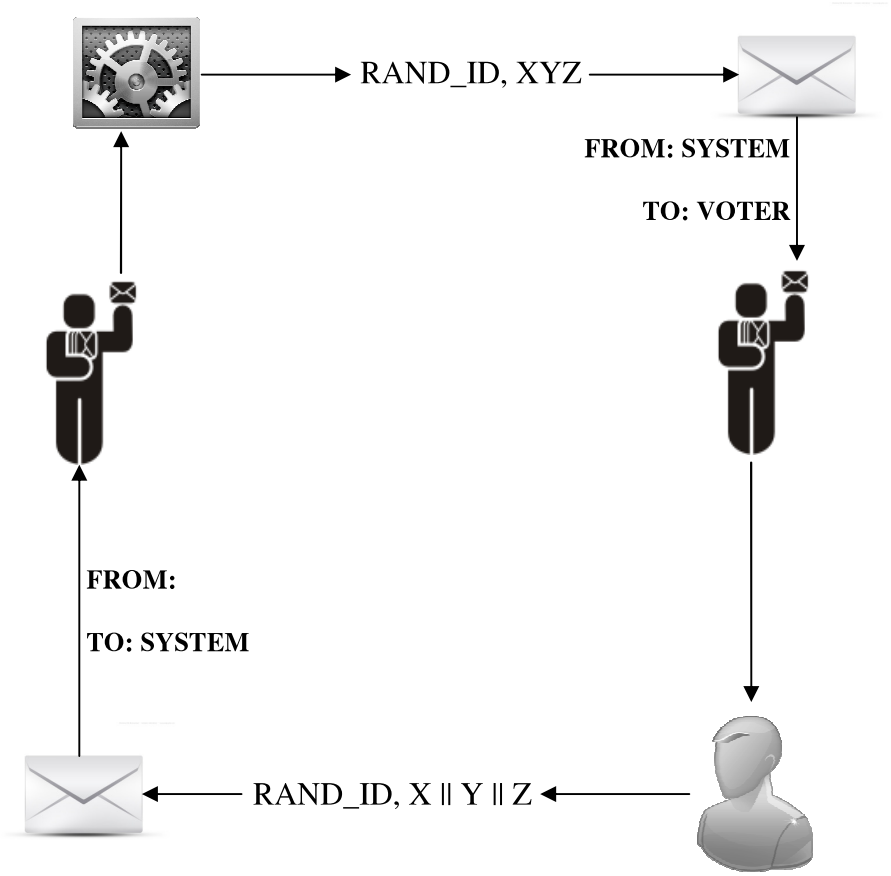
Tegyük fel, hogy Budapest egyik kerületének vezetése szavazásra bocsájtja az alábbi binárisan megválaszolandó kérdést: „Ön hozzájárul, hogy a kerületben a nyár folyamán meleg büszkeség felvonulás legyen rendezve?” Tegyük fel, hogy Gipsz Jakabnak határozott, de nem publikus véleménye van a kérdéssel kapcsolatban, s elmegy szavazni. Mivel a szavazási implementáció nem támogatja a szavazás tényének rejtését, így tegyük fel továbbá, hogy Gipsz Jakab főnöke direkt vagy áttétes úton információt szerez a szavazási esemény megtörténtéről. Ebben az esetben, amennyiben a munkáltató rossz véleménnyel rendelkezik mindkét szavazóbázisról, a megszerzett információ, függetlenül Gipsz Jakab véleményétől, hátrányos megkülönböztetés alapjául szolgáltat. Az információ hiányában az eseménytér háromelemű: igenlő szavazat, nemleges szavazat, nincs szavazat. Amennyiben nem teljesül az észlelhetetlenség kritérium, ez már csak kételemű, azaz a munkáltató biztos lehet benne, hogy az alkalmazott vagy igennel, vagy nemmel válaszolt. Igenlő válasz esetén a munkáltató az adott közösség tagjának vagy a közösséggel erősen szimpatizálónak tekintheti az alkalmazottat, nemleges válasz esetén pedig homofóbnak tarthatja, tehát tényleg szükségtelen a szavazás során adott válasz ismerete a hátrányos megkülönböztetéshez.

Szteganografikus megoldás esetén nincs szükség magas kapacitásra, hisz a legtöbb szavazás válasza akár egy biten is tárolható. Az alacsony kapacitásigény kedvező az észrevétlenségre s a robusztusságra nézve. A probléma ellenben az, hogy a szteganográfia akár magas absztraháltságú, legalapvetőbb alkalmazása is megkövetel bizonyos mértékű szakmai ismereteket. Az implementációt segítő szoftverek természetesen nem kerülhetnek szóba, hisz szigorúan nem elektronikus, tradicionális szavazórendszerekről van szó.

Szavazási helyszín tekintetében sem triviális a helyzet, hisz a központilag kijelölt helyszínre való megérkezés már magában hordozza a rejtendő információt, a „jaj, csak elkísértem egy ismerősömet” magyarázat pedig olyan átlátszó, mint az 1x1 pixeles .GIF webpoloska. Ebből kifolyólag a lehetséges megoldások eléggé le vannak szűkítve.

Egy lehetséges megoldás, ha mondjuk vesszük a fent említett példát, hogy minden szavazásra jogosult polgár postai úton kap egy levelet. Tegyük fel, hogy a postaszolgálat TTP-nek (Trusted Third Party) számít, innentől kezdve nincs szükség külön a megfigyelhetetlenség kritérium védelmére. A levél tartalmaz egy véletlenszerűen generált egyedi azonosítót, és egy háromjegyű számot, ahol minden számjegy különböző. A rendszer annyi véletlen karaktersorozatot és hozzá tartozó, nem szükségszerűen egyedi háromjegyű számot állít elő, ahány szavazásra jogosult személy van. Ezt követően a levéltartalmak egyesével borítékokba kerülnek. A folyamat ezen lépése után az összes lezárt boríték együttesen anonimitási halmazt képez, nem létezik olyan attribútum, mely akármelyiket megkülönböztetné a másiktól. Csak ezt követően

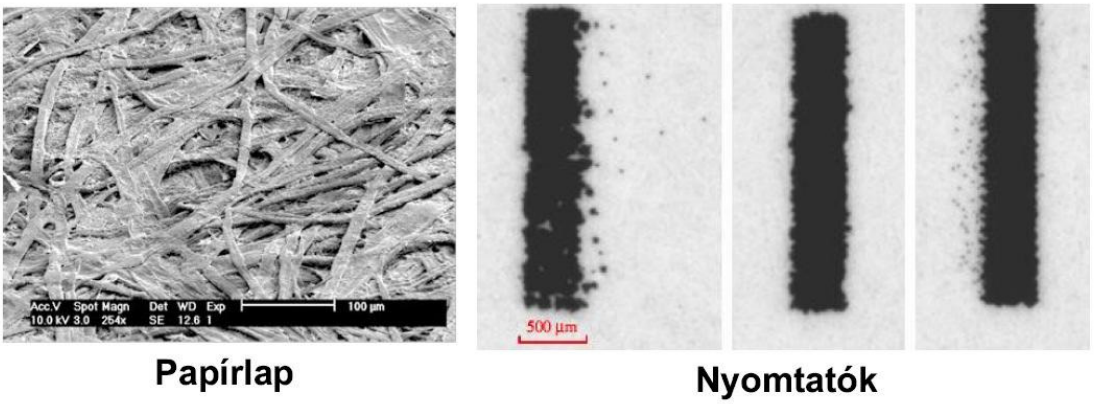
kerülnek megcímzésre a borítékok, így a rendszer által sem összepárosíthatóak a szavazók az azonosítókkal. Kiszállítás után a szavazó polgár abban az esetben, ha igennel szeretne válaszolni, akkor az első, ha nemmel, akkor a második, ha pedig nem óhajt véleményt nyilvánítani, akkor a harmadik számjegyet írja a válaszlevélbe az azonosítója után. A postaszolgálat a kiszállításhoz hasonlóan minden lehetséges szavazót egyesével meglátogat, és begyűjti a borítékokat, melyen a címzett a szavazást lebonyolító hivatal, feladó pedig nincs. A szavazatok feldolgozása során a rendszernek rendelkezésre áll az előállított azonosítók halmaza és a hozzátartozó számhármasok. A szavazat akkor érvényes, ha a megfelelő mezőket tartalmazza, az azonosító szerepel az adatbázisban, az azonosító után azon három szám egyike szerepel, ami ki volt adva, és egy adott azonosítóval csak egy válaszlevél érkezik. Egy rosszindulatú szavazó megteheti, hogy nem a kapott azonosítóját írja a válaszlevélbe, hanem véletlenszerűen egy másikat, megpróbálván ezzel egy szavazótársának érvényteleníteni a szavazatát. A szavazóbázishoz képest kellően hosszú azonosító választása minimalizálja az ütközés lehetőségét, emellett a támadónak el kell találnia azon három szám egyikét, ami az azonosítóhoz tartozik. Ami fontos, hogy nincs olyan szereplő a szavazási életciklusban, aki a szavazón kívül képes lenne az azonosítót párosítani a hozzátartozó személlyel, kivéve legfeljebb a postás, aki meg definíció szerint TTP.



4. ábra: Teoretikus szavazórendszer. A szavazói válasz második argumentuma vagy X, vagy Y vagy pedig Z értéket tartalmazza. A folyamat egyszeri lefutású, kezdete a rendszer kimenő éle. Egyszerre történik a szükséges véletlenkarakterek generálása, csomagolás, címzés, kiszállítás, válaszbegyűjtés, feldolgozás, nem pedig külön ciklus minden szavazóra.

A ma közismert tradicionális szavazórendszerek nem foglalkoznak az észlelhetetlenséggel. Példának véve a magyar parlamenti választási rendszert, választási lehetőségek színes palettáját nézve a szavazás ténye nem hordoz kritikus, védenivaló információt. Privátszféra tekintetében kizárólag az összeköthetetlenség s a teljes anonimitás a lényeges.

Ami korábban még nem került említésre a ma használt, papíralapú rendszerekkel kapcsolatban, hogy mennyire biztosít védelmet a szavazómédium. Az kellő magabiztossággal mondható, hogy két azonos tartalommal nyomtatott, azonos gyártó által előállított nyomtatópapír nehezebben megkülönböztethető, mint két törött cserépdarab. Tény, hogy elméleti síkon szóba kerülhet a nyomkövetéses profilírozás papír és nyomtató tekintetében.



5. ábra: Nyomkövetéses profilírozási lehetőségek papíralapú szavazómédium esetén.

Az ilyen jellegű profilírozás kivitelezéséhez eleve szükséges, hogy több, megkülönböztethető nyomtató legyen használva. A szavazólapok előállítása jobb esetben nem lokálisan történik, így marad a papírlapon keresztüli támadás. Szükséges ráfordított erőforrásokat tekintve a gyakorlatban inkább egy a szavazólap sarkára csempészett apró tollpötty preferálandó.

Ami a szavazórendszerek anonimitási halmazát illeti, merő tévhit, hogy a halmaz országos méretű. A valóság az, hogy erősen regionális. Ez különösen olyan településeknél fontos, ahol alacsony a lélekszám, azon belül is a szavazásra jogosultak száma. Az még tovább szűkíti a halmazt, hogy hányan mennek el szavazni, mennyi az érvényes szavazat. Megfelelő algoritmusokat és metainformációkat felhasználva akár azonosítási halmaz is előállítható adott bemenetre.

Vegyük például Pusztaapátit. A Központi Statisztikai Hivatal 2010-es statisztikái [1] szerint 29 fő él a településen, 24 lakásban. Mind a 29 fő szavazóképes. 2010. október 3-án önkormányzati választás [2] volt a településen. Bár a névjegyzékben hivatalosan 34 fő szerepelt, ebből az a helyi 29 mind meg is jelent s szavazott. Az egyéni listás választás négy jelöltje között helyenként csak 2-3 szavazatnyi különbség volt.

Tegyük fel, hogy a település egyik idősebb asszonyának, Babi néninek, a választás másnapján bauxit főzelék főzés közben hirtelen egyik pillanatról a másikra sürgős profilírozhatnékja támad. A jelöltek közül nagyon nem szimpatizált Károllyal, így szeretné megtudni ki volt az a 9 ember, aki rá szavazott, emellett furdalja az oldalát, hogy nagy riválisa, Golyvás Irén mégis kire szavazhatott. A kiindulási pont egy 28 fős anonimitási halmaz, mivel Alzheimer-kór hiányában még tudja kire szavazott azelőtti nap. Első lépésként felhasználja a rendelkezésre álló adatbázist, azaz kiről tudja, hogy kire szavazott, s fürgén halmazredukciót végez. Az így kapott anonimitási halmazt tovább szűkíti azáltal, hogy tudja, ki az, aki biztos nem szavazott Károlyra. Ezt az információ típust a többi jelöltre is alkalmazza, s próbál azonosítási részhalmazokat létrehozni, egészen addig, amíg el nem jut Irénhez. Időközben igyekszik az adatbázist bővíteni jól bevált verbális algoritmusokkal. Ezen felül próbálja felhasználni a rendelkezésre álló részidentitásokat, a Nexus Identity Networks alapú skizofrén szavazók esetén. A szavazáson mindenki megjelent s az egyéni listás választáson minden szavazat érvényes volt, de amennyiben nem így lett volna, az ezzel kapcsolatos információk s metainformációk is nagy segítséget kínálnának.

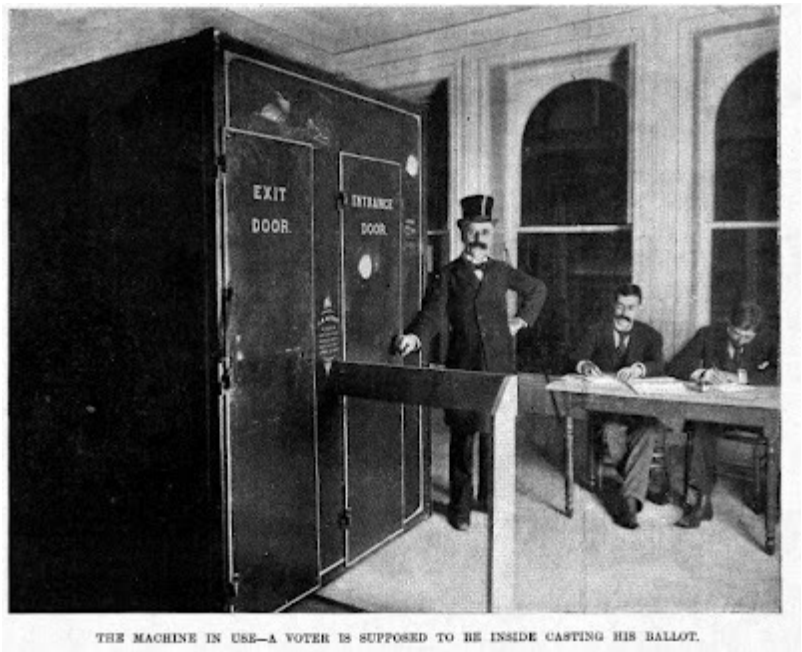
Tanulság, hogy egy tradicionális szavazórendszer esetén hiába jól megtervezett az eljárás, önmagában csak azt garantálja, hogy közvetlenül a rendszer nem sérti meg a szavazó privátszféráját, vagy nem ad lehetőséget mások számára, hogy pusztán a rendszer által biztosított információk és támadási lehetőségek alapján tudjanak párosítást végezni. Egy rendszer tervezésekor figyelembe kell azt is venni, hogy várhatóan milyen bemeneten fog a rendszer futni. A részletes statisztikák kellően kicsi bemenet mellett sokat segíthetnek privát információk kinyerésében.

Az előbbi példához még hozzátartozik, hogy nem pusztán akkor sérül a célszemély privátszférája, ha bizonyítható, hogy kire szavazott. Ahogy az korábban említve lett, az sem elfogadható állapot, ha a lehetőségek halmazának csökken az elemszáma vagy pedig egyenletestől eltérő valószínűségek rendelhetőek az elemekhez. Ilyen például, ha Babi néni meg tud határozni a Károlyra szavazók csoportjának tekintetében egy olyan enumerációt, mely létszáma megegyezik a Károlyra leadott szavazatok számával. Amennyiben ebben a listában nem szerepel Irén, Babi néni biztos lehet benne, hogy nem Károlyra szavazott.

3 Esettanulmányok

A szavazási rendszerek közül az egyik leginkább kiemelkedő implementáció Jacob H. Myers automata szavazófülkéje [3]. Legelsőnek 1892-ben került bevetésre, de egy évszázaddal később is még megállta a helyét az amerikai elnökválasztáson, kisebb áttervezésekkel és fejlesztésekkel természetesen. Igazi technológiai áttörésnek számított; saját korában csúcstechnológia volt, több mozgó alkatrésszel, mint akármilyen más akkori gépezet.

Népszerűségét és gyors terjedését annak köszönhette, hogy gyakorlatilag kizárta a szándékos választási csalás lehetőségét. A szavazópolgár a fülkébe lépve a jelöltjének megfelelő kart húzta meg, ami mechanikusan inkrementálta a jelölthöz tartozó szavazatok számát. A kar meghúzása után a rendszer blokkolt állapotba került, azaz másik kar meghúzása nem volt lehetséges. Távozáskor történt meg konkrétan a jelöltre leadott szavazatok számának növelése, miközben a meghúzott kar visszaállt kiindulási helyzetébe. Ez a megoldás nem pusztán a szavazó dolgát könnyítette és gyorsította meg, hanem a választási bizottságét is, hisz a nap végén a leadott szavazatok szavazóállomásonként már eleve meg voltak számolva. Ezen felül nem volt olyan értelmezve, hogy érvénytelen szavazat; egy kar meghúzásának műveletét elrontani semmiképp sem egy triviális, könnyű feladat. A kar, ha rendesen meg lett húzva, akkor a többitől eltérő, fix pozícióba került, ha nem, akkor pedig a többivel azonos állást, a kiinduló állapotot vette fel. Ehhez képest egy papír alapú szavazásnál egészen könnyű érvénytelen szavazatot generálni, például több jelölt kiválasztásával, a jelölésre szolgáló szimbólum nem megfelelő helyen történő elhelyezésével, vagy esetleg a kijelölt választható szimbólumok helyett virág rajzolásával. Kiegészítő információ, hogy szavazati jogukkal élni óhajtó nők számára a választás napja előtt már el voltak helyezve szavazógépek, melyeken gyakorolni lehetett.



THE MACHINE IN USE—A VOTER IS SUPPOSED TO BE INSIDE CASTING HIS BALLOT.

6. ábra: Myers automatizált szavazófülkéje. A képen látható kiindulási méret idővel csökkent, mely a fülke mobilitását segítette elő; a későbbi verziók könnyen szétszedhetők és szállíthatók voltak.

A hibák lehetősége természetesen nem volt teljesen kizárva. Elég abból kiindulni, hogy a gépezet számtalan mozgó alkatrésszel bírt, melyek meghibásodásra voltak hajlamosak, például a számláló beragadása. Arról nem is beszélve, hogy a karbantartók, amennyiben nem teljesen TTP-k voltak, akár módosíthattak is a választás helyi eredményén. Az évek folyamán a rendszer folyamatos fejlesztés alatt volt, hogy minél kevésbé legyen hajlamos a rendszer a szavazás pillanatában történő észlelhetetlen meghibásodásra, emellett az is fontos szempont volt, hogy növekedjen az eszköz mobilitása. Egyértelmű, hogy dizájn és ergonómiai tekintetekben is fejlődött, ahogy változott a világ. Változott a színvilág, a formavilág, a térkihasználás, sőt az sem kizárható, hogy egyes variációknál halk zene szólt, mint ahogy az a felvonókra jellemző. Nincs is ideálisabb, mint mikor szavazás közben szól a PET Shop Boys.

Privátszféra tekintetében is elég kedvező a rendszer. A szavazatok sorrendje nem kerül tárolásra, mindössze a szavazás ténye s a szavazati döntés. A szavazók közös médiumot használnak különböző időpontokban. A szavazás pillanatában a szavazó garantáltan egyedül volt, külön őr ügyelt arra, hogy egyszerre csak egy emberben fáradjon be a helységbe. Más nem láthatta a karok állását, hisz távozáskor automatikusan alapállapotba került a felhasználói felület. Ami esetleg információszivárgásra adhat egy ilyen rendszerben lehetőséget az maga a kar. Mivel nem minden embernek azonosan magasak a kézhigiéniai szükségletei, így a nap vége fele a karok külső megjelenése alapján lehetett következtetni a szavazatok eloszlására. Egyszerűbb eset, ha egy autószerelő, egy bányász, egy kéményseprő vagy egy olyan ember megy el szavazni, kinek szakmája tapad a kezéhez. A szavazat leadása s távozás után az őt követő szavazó láthatta, hogy éppenséggel melyik jelölthöz tartozó kar lett mondjuk kicsit gépolajos.

A tradicionális anonim szavazási rendszerek közül a lyukkártyás rendszerek [4] említésre méltóak, alkalmazásra már kevésbé. Az egész Votomatic technológia a korszak erőltetett szülötte. Rendelkezésre állt egy jól működő, kiforrt, letisztult szavazási rendszer. Pont azért, mivel a meglévő rendszer már régi volt úgymond, s a lyukkártya trend terjedőben volt világszerte, egyes emberek szükségét érezték, hogy létrehozzanak egy olyan új rendszert, ami akár akkora áttörés lehet, mint Myers szavazógépe. Nem, nem lett az. Tény, hogy az 1996-os amerikai elnökválasztáson [5] több szavazatot adtak le lyukkártyás gépen, mint hagyományos mechanikus szavazógépen, mégis az évek során sokkal több negatív kritikát kapott. Ennek ellenére egyes helyeken még ma is hagyományőrzően alkalmazzák, például Los Angeles.

„*The Votomatic was an invention that made voting easier only for people who have trouble making an "X" in a box.*”[6]

- The New York Times

Azaz a lyukkártyás Votomatic szavazógép oly találmány volt, mely kizárólag azon emberek számára könnyítette meg a szavazást, kiknek egy négyzetbe történő ikszelés gondot okoz. Szerintem itt a szó már kevés. Nyelvezeti korlátaim miatt egyszerűen nem tudom az arckifejezésem hordozta információt méltó módon visszaadni puszta szavak segítségével. Az mondjuk elképzelhető, hogy az ezen halmazba tartozó embereknek tényleg szükségük volt a Myers gépén történő karhúzás gyakorlására.

A tisztán elektronikus szavazási rendszerek megjelenése előtt szkenner típusú szavazórendszerek [7] is léteztek s működtek. Gyakorlatilag megfeleltethető a ma ismert tradicionális papíralapú szavazórendszernek, azonban a hazárd kedvéért a feldolgozás nem pusztán humánerőforrásra volt alapozva; a szavazatok beolvasását és összeszámolását egy számítógép végezte. Egy szám inkrementálása nem okozott már akkor se gondot egy számítógép számára, főleg, hogy egy szavazókörzetben egy adott jelöltre leadott szavazatok száma várhatóan nem haladta meg a számábrázolási korlátot. A humán faktor azonban magában hordozta azt a komplikációt, hogy a szavazó által a szavazási ellipszisben elhelyezett jelölés nem feltétlenül volt megfelelő a számítógép számára. Ne feledjük el, olyan világban élünk, ahol a szavazóképességnek nem szükséges kritériuma az ikszelési kompetencia.

Amennyiben a szavazó húz egy határozott vonalat az ellipszis belsejében, mely megközelíti az ellipszis szélességét, jó esély van rá, hogy a számítógép érvénytelennek minősíti a szavazatot. Amennyiben ez a vonal egy picit is kilóg az ellipszisből, már biztos érvényes szavazatként könyveli el. Ha valaki netán úgy dönt, hogy bekarikázza az ellipszist, annak is számolnia kell azzal, hogy szavazata valószínűleg érvénytelen. Ugyanez vonatkozik azokra, akik egy határozott pöttyöt raknak az ellipszis közepébe vagy satíroznak. Satírozás esetén, ha a teljes ellipszis 000000000000000000000000 feketével kerül kitöltésre, azaz még egy szteganografikus egyes se férne be az LSB-be, a szavazó biztos lehet benne, hogy a toll vagy ceruza feláldozását a számítógép egy érvényes szavazattal hálálja meg.

Első ránézésre privátszféra tekintetében a rendszer nem különbözik a sima papíralapú szavazástól. Gyakorlatilag ugyanaz az eljárás, annyi különbséggel, hogy nem emberek dekódolják, érvényesítik és számolják a szavazómédiumokat, hanem egy számítógép. Tény, hogy a feldolgozás kivételével nincs semmi különbség, ám pont ez akár lehetőséget adhat privát információk megsértésére. A számítógép akár rögzíthet feldolgozási sorrendet egy log fájlban. Amennyiben a szavazás megkezdése előtti hitelesítés során is rögzítésre kerül az érkezési sorrend, már csak a szavazó urnán múlik, hogy véghez vihető-e könnyedén párosítás.

Érvényességi jellemzőként korábban láthattuk, hogy pusztán egy pont elhelyezése az ellipszisben nem számít érvényes szavazatnak. Tegyük fel, hogy az adott szavazó kezdetben véletlenül rossz ellipszist céloz meg írószerszámával, melynek hegyének lehelyezésekor tudatosul benne hibája, s még időben átvált a megfelelő ellipszisre. A szavazási központ elhagyása előtt puszta lelkiismeretességből rákérdez a jelen lévő szavazóhatóság egyik tagjára, hogy ilyen esetben érvényesnek tekinthető-e egy ilyen szavazat, tehát ahol az egyik ellipszis egy pontot, a másik pedig egy rendes ikszet tartalmaz. Abban az esetben, ha az adott illető volt az egyetlen, aki efféle jelölést végzett, szavazólapja alapján azonosítható s egyértelműen meghatározható, hogy kire szavazott.

Az összes nem elektronikus szavazórendszerre jellemző, hogy a szavazó nem tudja szavazatának feldolgozását nyomon követni, nem kap semmilyen bizonyítékot, mely igazolná, hogy szavazata megfelelően fel lett dolgozva és be lett számítva. Ez azonban nem feltétlenül rossz dolog.

Tételezzük, hogy adott kötőtűipari vállalatok csoportjának közös érdeke, hogy közterületen lehessen pulóvert és sálat kötni. A törvényhozói hatalom tagjai névtelen szavazás keretén belül döntik el, hogy közterületen való kötögetés jogszerű cselekménynek számítson vagy pedig pénzbüntetést, esetleg letöltendő szabadságvesztést vonjon maga után. A szavazás előtti napon a vállalati csoport egy küldöttsége felkeresi a szavazóbizottság egy tagját, s megkérik, hogy a szavazáson számunkra megfelelően szavazzon, melyet adott pénzösszeggel vagy értékes kötőtű szállítmánnyal honorálnának. Amennyiben a szavazónak lehetősége lenne szavazatát igazolni, megtehetné, hogy a szavazás után felveszi a kapcsolatot a korábban említett küldöttséggel, s prezentálja számukra a szavazatát igazoló iratot, melyet követően átvenné tiszteletdíját. Azonban ha szavazatának igazolására nincs lehetősége, rögtön olyan komponens megléte igényeltetik a rendszerben, mely ritka, mint a gyors szteganografikus fájlrendszer. Ez pedig nem más, mint a bizalom.

4 Összefoglalás

A tradicionális anonim szavazórendszerek elsődleges célja, hogy precízen tükrözze a szavazók akaratát, ugyanakkor legalább olyan fontos, hogy a szavazás teljes életciklusa alatt megőrizze a szavazó anonimitását. Törekedni kell a teljes anonimitás megőrzésére, azaz nem pusztán a szavazat és szavazó összepárosítás lehetőségét kell kizárni, hanem a célhalmaz szűkítését vagy az egyes elemekhez történő súlyozást is. Oda kell figyelni metainformációk és statisztikák publikálására, melyek akár nagy segítségül szolgálhatnak privát információk gyűjtésében, előállításában. Adott esetben akár maga a szavazás ténye is rejtendő információ lehet.

Az évek során a legkülönfélébb szavazórendszerek kerültek bevezetésre. Bár tervezéskor mindig a szavazati csalások megakadályozása a fő szempont, némely implementáció, például Myers gépezete, tervezéséből adódóan közel tökéletes privátszféra védelmet biztosít. Magyarországon perpillanat a papíralapú szavazórendszer van működésben parlamentáris szavazások tekintetében, mellyel kapcsolatban bár megjelent olykor a választási csalás sötét árnyéka, nem veszélyeztette a szavazók privátinformációhoz való jogát. Fontos itt megjegyezni, hogy az esetleges szavazói adatbázisok [8], melyek komoly etikai és jogi kérdéseket vethetnek fel, nem a szavazórendszer implementációs hiányosságaiból álltak elő.

A szavazók információinak védelme több szervezet [9] számára is kardinális kérdés. A szomorú ezzel kapcsolatban az, hogy az esetek nagy részében az efféle szervezeteket sokkal jobban érdeklik a szavazópolgárok privátszférájának védelme, mint magát a szavazót.

Irodalomjegyzék

Az esszé megírásához szükséges elméleti anyag alapja a http://course.pet-portal.eu/ oldalon található oktatási diasorok.

[1] http://www.ksh.hu/docs/hun/hnk/hnk2010.pdf

[2] http://valasztas.hu/dyn/ov10/outroot/onktjk5/20/tjk20173.htm

[3] http://www.divms.uiowa.edu/~jones/voting/pictures/#lever

[4] http://americanhistory.si.edu/vote/punchcard.html

[5] http://inventors.about.com/library/weekly/aa111300b.htm

[6] http://www.nytimes.com/2000/12/04/opinion/the-age-of-the-votomatic.html

[7] http://www.divms.uiowa.edu/~jones/voting/OpticalMarkSenseScanning.pdf

[8] http://hvg.hu/itthon/20100407_fidesz_kubatov_gabor

[9] http://epic.org/privacy/voting/

Ábrajegyzék