ANALOGICO E DIGITALE: OBBLIGHI, DIRITTI E CERTEZZE

SICUREZZA DEI SISTEMI DI VOTO ELETTRONICO

CORRADO GIUSTOZZI

ENISA/PSG

I punti che tratterò

- Democrazia e processo di voto:
  - obiettivi del processo di voto: verificabilità e segretezza
  - requisiti del processo di voto: sicurezza e fiducia
- Automazione del voto:
  - requisiti
  - tipologie
- Voto elettronico:
  - problemi, rischi
  - vulnerabilità
  - possibili approcci

DEMOCRAZIA E PROCESSO DI VOTO

UN BREVE EXCURSUS STORICO

Considerazioni generali

- La democrazia dipende dalla corretta gestione del voto, in quanto espressione della volontà popolare
- Il processo di voto è una faccenda complicata, che cerca di raggiungere obiettivi spesso discordanti:
  - ogni votante dovrebbe ottenere sufficienti garanzie del fatto che la sua intenzione sia stata correttamente registrata e che tutti i voti legittimi siano stati contati
  - il sistema di voto dovrebbe minimizzare i rischi di coercizione dei votanti, perfino in situazioni nelle quali gli stessi votanti sarebbero disponibili ad essere influenzati
- Ogni votante dovrebbe avere abbastanza informazioni per fidarsi del processo ma non abbastanza per provare il proprio voto ad altri!

Breve storia del voto (1/2)

- Il voto come oggi lo conosciamo è un'invenzione piuttosto recente, soprattutto per quanto riguarda il requisito della segretezza delle preferenze
- Il primo esempio documentato di votazione risale all'antica Grecia, ma aveva valenza negativa:
  - ogni politico che riceveva più di 6.000 "nomine" veniva esiliato per dieci anni (ostracismo)
  - in generale i greci consideravano il voto "poco democratico" in quanto favoriva i candidati noti e famosi
- Il primo voto per approvazione venne introdotto a Venezia nel XIII secolo per la scelta del Doge:
  - il processo era tuttavia molto complicato, ed includeva collegi elettorali multipli ed estrazioni a sorte

Breve storia del voto (2/2)

- Negli USA il voto fu a lungo piuttosto primitivo:
  - fino al 1800 il voto era **orale** e **pubblico**: il votante dichiarava ad alta voce la sua preferenza di fronte agli scrutinatori, che ne prendevano nota in copie multiple
  - nei primi anni del 1800 vennero introdotte le **schede elettorali**, prodotte dal votante stesso o dai partiti politici
  - in seguito sorse l'uso di rifornire i seggi con due serie di schede prestampate (repubblicani e democratici), da cui l'elettore prendeva e consegnava quella di sua scelta
- Il primo voto segreto con criteri moderni fu introdotto nel 1858 in Australia e prevedeva:
  - schede stampate e distribuite a cura dello stato
  - compilazione anonima all'interno di cabine chiuse

Requisiti contraddittori (1/2)

- Un moderno sistema di voto deve poter garantire due proprietà fondamentali ma contrastanti tra loro:
  - **verificabilità** del processo di voto
  - **segretezza** del voto espresso
- La **verificabilità** ha lo scopo di evitare brogli:
  - consentendo di assicurarsi del regolare andamento del processo di voto e/o di accertarlo a posteriori
  - permettendo, in caso di dubbi o contestazioni, di effettuare un riconteggio delle preferenze espresse
- La **segretezza** ha lo scopo di eliminare indebite pressioni esterne sugli elettori:
  - chi vota può esprimere più liberamente la sua preferenza sapendo che nessuno potrà mai conoscerla

Requisiti contraddittori (2/2)

- La **verificabilità** si ottiene mediante:
  - la suddivisione di compiti e responsabilità fra più parti
  - l'effettuazione di controlli e verifiche incrociate fra le parti
  - la tenuta di verbali e registri delle operazioni svolte
  - l'adozione di misure di sicurezza fisica a protezione
  - la conservazione nel tempo di verbali, registri e schede
- La **segretezza** si ottiene mediante:
  - il disaccoppiamento fisico tra il votante (identificato e autorizzato) e la sua preferenza (scheda anonima)
- È impossibile ottenere contemporaneamente una perfetta verificabilità ed una perfetta segretezza!
  - ogni sistema è solo un compromesso fra le esigenze

Sicurezza e fiducia

- I due pilastri su cui si fonda l'affidabilità di un sistema di voto sono **sicurezza** e **fiducia**
- La **sicurezza**, attuata mediante l'adozione di misure fisiche di protezione su locali, documenti (schede, registri) e oggetti (urne), previene eventuali azioni fraudolente da parte di chiunque tese ad alterare il regolare andamento delle operazioni di voto e/o di conteggio delle preferenze espresse dai votanti
- La **fiducia**, attuata mediante la trasparenza del processo, la separazione delle responsabilità e l'attuazione di controlli incrociati, previene eventuali azioni fraudolente da parte dei gestori del sistema

Automazione del processo di voto

- Il termine è ambiguo: occorre distinguere tra due situazioni molto diverse:
  - automazione dell'intero processo di espressione della preferenza elettorale (voto vero e proprio): **difficile**
  - automazione della sola fase di conteggio delle preferenze espresse in modalità tradizionale (scrutinio): **più facile**
- Da sempre, soprattutto negli USA, si è cercato di sviluppare sistemi automatici per la gestione delle elezioni che garantissero:
  - efficienza ed efficacia del processo di voto
  - i principi fondamentali di verificabilità e segretezza

Le prime macchine per votare

- La prima proposta di usare macchine per gestire le elezioni in modo sicuro venne dai Cartisti nel 1838
  - primi brevetti: 1875 (Spratt), 1881 (Beranek)
  - primo utilizzo: 1892 (New York)
- Si trattava di congegni meccanici che, impostando una scelta mediante leve o pulsanti, facevano avanzare uno solo fra diversi contatori odometri:
  - il processo di voto si svolgeva all'interno di una cabina che non consentiva di vedere l'azione del votante
  - la macchina si bloccava dopo ogni azione di voto
  - la porta della cabina era collegata alla macchina in modo da riportarla alla posizione iniziale ad ogni apertura
  - i contatori rimanevano nascosti sino alla lettura dei totali

SVMC, New York, circa 1890

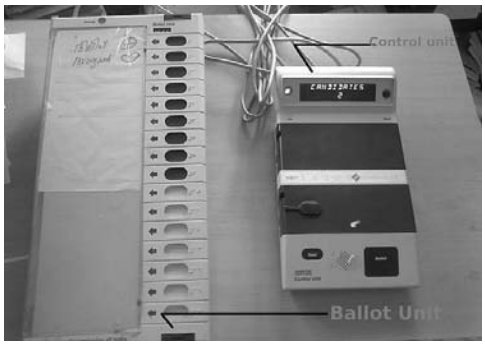
- Macchina progettata da Alfred J. Gillespie e commercializzata dalla Standard Voting Machine Company di Rochester, New York, a partire dalla fine degli anni 1890
- Utilizzata per decenni

Un utilizzo durato oltre un secolo

Shouptronic, oggi

- Macchina elettromeccanica contemporanea prodotta da Shouptronic prendendo a modello le macchine a leve
- Dotata di touch-screen, registra i voti su un hard disk locale

India, oggi



Il voto on-line

Le elezioni al tempo di Internet

Diverse tipologie di voto on-line

- Occorre fare attenzione al fatto che non tutti i sistemi di e-democracy sono e-vote (e viceversa!)
- Valore (e requisiti) molto differenti tra atti diversi:
  - consultazione on-line
  - elezioni on-line
- Per una semplice consultazione, o un'elezione non generale e/o non politica (ad esempio una primaria di partito) molti requisiti di sicurezza e riservatezza possono essere attenuati:
  - di solito si può dare fiducia al gestore
  - sono da temere più gli errori in buona fede che i brogli
  - la segretezza del voto non è sempre così importante

Proprietà e requisiti del e-voto

- Il meccanismo di e-voto deve poter garantire varie proprietà fondamentali, alcune ovvie ed altre meno
- Proprietà sempre necessarie:
  - solo gli aventi diritto devono poter votare
  - nessuno deve poter votare più di una volta
  - nessuno deve poter stabilire per chi hanno votato gli altri
  - nessuno deve poter duplicare il voto altrui
  - nessuno deve poter modificare o cancellare il voto altrui
  - ogni votante deve poter essere sicuro che il suo voto sia stato regolarmente acquisito e conteggiato nel totale
- Talvolta è anche desiderabile che:
  - ognuno possa sapere chi ha votato e chi no

Possibili soluzioni

- Ancora non esiste una soluzione perfetta!
- Tutte le soluzioni ad oggi proposte per evitare che il gestore del sistema possa imbrogliare si basano sostanzialmente su uno di questi due approcci:
  - non si può evitare che il sistema sia gestito da una sola entità, quindi esso va dotato di sicurezze intrinseche che necessariamente dipendono in larga parte dall'abilità dei votanti di svolgere un ruolo attivo nel processo
  - si fa in modo che il sistema venga gestito da *due* entità separate, equipotenti e possibilmente in concorrenza, organizzando i processi in maniera tale che nessuna delle due abbia sufficienti capacità, agendo da sola, di truffare senza essere scoperta dall'altra o dai votanti

Approccio a gestore unico

- Si basa fortemente sull'uso esclusivo di moderne e sofisticate tecniche crittografiche per poter fornire in modo oggettivo sicurezza e fiducia al processo:
  - blind signatures
  - zero-knowledge proofs
- L'idea è dare ad ognuno (gestore e votanti) un numero di informazioni sufficiente a garantire alcune certezze senza però rivelare troppi dettagli
- In questo modo può essere prevista una sola entità di gestione del sistema, a patto però che ogni votante possa compiere sofisticate elaborazioni
- Sistemi del genere sono assai complessi e delicati

Approccio a doppio gestore

- Non utilizza intrinsecamente tecniche di crittografia ma si basa su una accurata distribuzione di ruoli e responsabilità e su un attento disegno del processo:
  - nessuno dei due gestori possiede sufficienti informazioni per poter imbrogliare da solo senza essere scoperto
  - per poter imbrogliare dovrebbero colludere, ma in questo caso l'imbroglio verrebbe scoperto dai votanti
- L'idea è dare ad ognuno (gestori e votanti) un numero di informazioni sufficiente a verificare l'operato degli altri ma non ad imbrogliare da solo:
  - chi autentica i votanti non conta i voti e viceversa
- Consente sistemi più semplici, potenzialmente idonei ad un utilizzo via Web (ma non via mail!)

Problemi specifici

- Il funzionamento del processo è di per sé opaco:
  - il software non è facilmente ispezionabile
  - le funzioni implementate sono sofisticate e complesse
  - come assicurarsi che non ci siano errori o backdoor?
  - come assicurarsi che il software ispezionato sia davvero quello che viene eseguito?
  - il conteggio centralizzato dà molto potere al gestore!
- Il sistema è delicato perché complesso e articolato:
  - hardware e software che interagiscono a molti livelli
  - sicurezza delle comunicazioni, della memorizzazione, …
- I sistemi sono sempre vulnerabili ad attacchi!
- È assai più difficile assicurare sicurezza e fiducia

Conclusioni

Considerazioni e commenti finali

Considerazioni finali

- Un sistema di e-vote è per sua natura **complesso** e **poco trasparente**, ed è difficile sia costruirlo correttamente che dimostrarne le proprietà di:
  - sicurezza *interna* (mancanza di *bug* e di *backdoor*)
  - sicurezza *esterna* (resistenza ad attacchi)
- Conseguenze di questa situazione:
  - è necessario (ma non sufficiente) che il sistema si basi su piattaforme aperte, con software libero ed ispezionabile
  - è necessario adottare processi trasparenti e verificabili
- Occorre comunque **fiducia** nel gestore:
  - i rischi dovuti alla eventuale mala fede del gestore si possono ridurre ma mai eliminare completamente!

Alcune posizioni importanti

- Nel 2009 l'Olanda ha proibito il voto elettronico dopo che un'apposita commissione di esperti formata su incarico governativo ha stabilito che i sistemi attualmente in uso sono ancora troppo insicuri, e che sviluppare un sistema realmente sicuro sarebbe troppo costoso rispetto al costo della gestione tradizionale delle elezioni su carta
- Nel 2009 in Germania la Suprema Corte ha stabilito che il voto elettronico è incostituzionale in quanto non si può pretendere che il cittadino medio sia in grado di comprendere esattamente i passi necessari per acquisire e conteggiare i voti

Concludendo…

- Fare click su un form per scegliere un candidato non è un'elezione, più di quanto non lo sia chiedere a voce un voto a persone scelte a caso per strada!
- Un sistema elettorale idoneo a gestire elezioni politiche deve essere a prova di tutti e verificabile da tutti, compresi i gestori e gli stessi votanti
  - in particolare chi vota deve poter verificare che il suo voto sia stato regolarmente acquisito e conteggiato nel totale
- Non ci si può fidare di sistemi:
  - chiusi, basati su meccanismi proprietari e non noti
  - gestiti in proprio da un'unica organizzazione
  - non pubblicamente testati da esperti (*peer review*)

Analogico e digitale: obblighi, diritti e certezze

Grazie per l'attenzione

Sicurezza dei sistemi di voto elettronico

c.giustozzi@acm.org