PROJECT WORK – Algoritmi e Protocolli per la Sicurezza

L.M. Ingegneria Informatica

Docenti: V. Iovino - I. Visconti

A.A. 2021-2022

(versione del 13 Aprile 2022)

Premessa. Durante la pandemia alcune elezioni sono state rinviate per la pericolosità del voto al seggio. Inoltre, il voto in presenza al seggio è costoso in quanto richiede una miriade di seggi distribuiti capillarmente sul territorio (il che mitiga attacchi su larga scala), ciascuno con personale adibito alle operazioni di voto e forze dell'ordine per questioni di sicurezza. Lo spoglio su singolo seggio condiziona negativamente la privacy (es., in alcune elezioni ci sono candidati che prendono pochissimi voti, anche zero, in un seggio e quindi si può dedurre che alcuni che votano in quel seggio non hanno votato per un certo candidato). Inoltre, non c'è la privacy di chi decide di non votare. Ci sono spesso interpretazioni fuorvianti nello spoglio ed altre anomalie (schede mancanti) che inficiano la correttezza del risultato. C'è in generale la difficoltà di controllare la possibilità che il votante registri/fotografi l'azione svolta nell'urna per avere una ricevuta da esibire a terzi. In aggiunta c'è il problema progressivamente crescente che gli elettori ormai non vivono permanentemente nei pressi del luogo di residenza, la società si evolve favorendo la mobilità. C'è il voto (in Italia) dei residenti all'estero che è disciplinato mediante voto via posta, che è scarso in termini di garanzie e di recente è stata revocata l'elezione di un parlamentare eletto all'estero. Prima o poi si finirà col votare nel metaverso.

Mentre alcune nazioni (es. Estonia) hanno già da anni stabilito meccanismi di voto elettronico/remoto, altri governi (quello italiano incluso) stanno timidamente avviando delle sperimentazioni nel tentativo di mitigare alcune criticità quali ad esempio il voto via posta ed il voto di chi è impossibilitato a recarsi al seggio in quanto per lavoro/studio si trova altrove.

Ci sono varie insidie che riguardano il voto elettronico/remoto alcune delle quali dipendono dal tipo di voto. Ovviamente si vuole che il conteggio dei risultati sia corretto. Spesso il voto deve restare segreto, nel senso che chi vota dovrebbe avere la tranquillità che la sua identità non sia in futuro associata alla preferenza che ha espresso. Un'altra proprietà che può essere desiderata è evitare la coercizione, cioè permettere di votare liberamente malgrado ci sia qualcuno interessato a farci votare secondo le sue indicazioni. Chi vota vorrebbe poter controllare che il proprio voto sia stato contato correttamente. Il voto remoto deve ovviamente soddisfare requisiti di usabilità. Ovviamente un voto remoto/elettronico può essere sempre legato anche ad azioni svolte non elettronicamente (è naturale prevedere delle fasi che non sono elettroniche quali ad esempio l'ottenimento delle credenziali per votare).

Alcuni dei precedenti requisiti/desideri sono tra loro contrastanti e non è affatto chiaro che tutte le proprietà desiderate possano essere raggiunte in pieno. Del resto, anche il voto fisicamente al seggio e via posta sono altamente imperfetti. E' verosimile che un sistema di voto elettronico/remoto si regga su compromessi/assunzioni e vari meccanismi che provano a mitigare criticità sapendo che i rischi non sono evitabili in assoluto.

Inoltre, esistono vari tipi di voto (e.g., referendum, ballottaggi, elezioni con scelta del candidato e senza scelta, elezioni con pochi candidati per milioni di persone ed elezioni con vari candidati anche su comunità di poche migliaia di persone).

Ci sono anche gli oppositori dell'innovazione, ossia dinosauri che anziché studiare le nuove tecnologie non fanno altro che indicarne genericamente i rischi con il solo scopo di lasciare tutto così com'è, riferendosi a chi le studia col termine "tecnocrati". Sono in genere allarmisti che puntano sul fatto che tutti i dispositivi possono essere compromessi, la sicurezza assoluta non esiste, la democrazia è troppo importante e chi propone il voto elettronico ha forse l'obiettivo di abusarne le deficienze. Sono i no-evox.

Per evitare facili strumentalizzazioni da parte di tali complottisti è quindi necessario che un sistema di voto remoto/elettronico sia trasparente nel senso che non debba affidarsi eccessivamente ad una presunta parte fidata, ma abbia invece una progettazione ed analisi che permetta a tutti di verificarne la sua bontà limitando il danno che può essere causato da un qualunque avversario.

Obiettivo del project work: individuare un tipo di voto e realizzarlo permettendo il voto elettronico/remoto nel modo migliore possibile.

Ci sono 4 pilastri fondamentali da considerare:

- confidenzialità: i dati sensibili dovrebbero restare confidenziali anche in presenza di attacchi;
- integrità: il sistema dovrebbe realizzare la funzionalità prevista anche in presenza di attacchi;
- trasparenza: il sistema non dovrebbe essere basato su algoritmi segreti e la sua confidenzialità/integrità non dovrebbe essere legata ad un uso eccessivo di parti ritenute fidate per tutti i partecipanti; in presenza di assunzioni di fiducia verso alcune parti è necessario argomentarne le motivazioni concrete legate alla possibilità che eventuali abusi siano verosimilmente identificati e puniti in caso di frodi e a fattori psicologici quali il preservare la buona reputazione che scoraggiano tali abusi;
- efficienza: il sistema dovrebbe essere utilizzabile senza eccessivi costi e ritardi.

Da tenere conto:

- si può assumere che i dispositivi di chi è onesto non siano corrotti; quindi, che l'hardware non sia compromesso ed il software non sia controllato da malware/virus/trojans; è tuttavia richiesta una discussione su cosa può accadere in case contrario, e come si potrebbe provare a mitigare il problema;

- prestare particolare attenzione agli attacchi su larga scala (cioè attacchi che colpiscono molti voti/votanti) e considerare che la correttezza del risultato è prioritaria rispetto ad altre proprietà riguardanti la privacy e la coercizione;

- è naturale che vari avversari interessati a barare per scopi personali possano cooperare per avvantaggiarsene insieme; questo però potrebbe esporre rischi alla loro reputazione visto che non necessariamente si fidano gli uni degli altri; considerare quindi questi macro-avversari tenendo conto della concreta difficoltà del tenere in piedi una coalizione eterogenea;

- è fondamentale l'originalità del lavoro svolto; gli studenti devono accertarsi di avere completa padronanza di tutto il contenuto del project work che viene consegnato;

- la commissione non si aspetta project work che rivoluzionino l'e-voting, ma solo che gli studenti usino adeguatamente le conoscenze acquisite durante il corso per esibire un ragionevole modello (cioè funzionalità con parti oneste + threat models + proprietà di resilienza), una dignitosa soluzione, una attenta analisi ed una appropriata implementazione.

Struttura: il project work dovrà essere organizzato in 4 work packages. Tutte le scelte nei 4 work packages devono essere motivate, spiegate/illustrate e documentate.

WP 1: Modello

Questo work package si occuperà di definire i vari attori onesti del sistema e i loro obiettivi specificando quindi la funzionalità che si intende realizzare. Dovranno essere poi discussi i possibili avversari (threat models) interessati a compromettere il sistema (specificando le loro risorse). Vanno identificate le proprietà che si vorrebbe poter preservare in presenza di attacchi. Il soddisfacimento della funzionalità e delle proprietà individuate permetterà poi di misurare (non in questo WP) la bontà di una progettazione che prova a realizzare un tale funzionalità in presenza di avversari.

Nota 1. 1: questo WP non deve mostrare una soluzione al problema.

Nota 1.2: è importante discutere in modo comprensibile, dettagliato e non-ambiguo la funzionalità che si vuole realizzare, i possibili obiettivi/attacchi degli avversari (incluse le loro risorse), le proprietà di resilienza del sistema in presenza di attacchi. Per ottenere il punteggio massimo non è necessario presentare definizioni formali (presentarne anche solo qualcuna è un plus).

WP 2: Soluzione

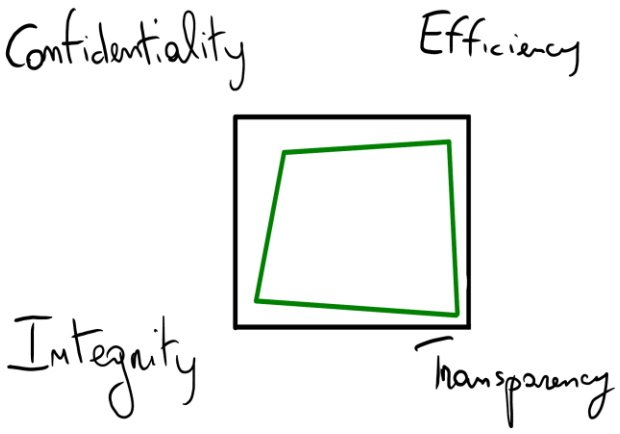
Dato il modello identificato in WP 1, mostrare un sistema di voto remoto/elettronico con l'obiettivo di raggiungere un ragionevole compromesso tra efficienza, trasparenza, confidenzialità e sicurezza. La progettazione deve descrivere dettagliatamente tutte le azioni delle parti oneste coinvolte nel sistema.

Nota 2.1: Questo WP non richiede di dimostrare che la soluzione proposta soddisfi le proprietà descritte in WP 1. La progettazione, quindi, non deve presentare attacchi eccetto che nel motivare/commentare/discutere le scelte progettuali si possono ove utile indicare le criticità che si prova a mitigare attraverso di esse.

Nota 2.2: Si richiede l'uso corretto degli strumenti studiati durante il corso, non è necessario individuare/studiare nuovi strumenti.

WP 3: Analisi

Questo work package ha lo scopo di analizzare la soluzione presentata in WP2 rispetto al modello presentato in WP1. Richiede inoltre di esibire e giustificare dettagliatamente un grafico radar (segue un esempio) i cui 4 vertici sono Efficienza, Confidenzialità, Integrità e Trasparenza. Gli studenti devono attentamente verificare che non ci siano ovvie modifiche apportabili a WP2 che portino benefici in alcune proprietà senza alcuna perdita in altre proprietà.



WP4: Implementazione e prestazioni

Implementare il sistema di voto remoto/elettronico progettato in WP 2 (anche solo una parte di esso se le funzionalità sono tante) in un ambiente simulato (ad es., cioè non è necessario sviluppare un'app per smartphone, la si può simulare mediante applicazione stand-alone in esecuzione su un computer). Utilizzare il linguaggio Java quando è necessario programmare. Mostrare anche le prestazioni ottenute con la sperimentazione.

Valutazione.

La valutazione massima del project work è di 12 punti (come indicato su esse3). Ogni work package è valutato da 0 a 3 punti e questo forma il punteggio di partenza assegnabile ai membri del gruppo supponendo che: a) gli studenti abbiano equamente contribuito al project work; b) gli studenti abbiano adeguatamente presentato il contenuto del project work durante il colloquio; c) il punteggio di partenza corrisponda anche alla qualità del lavoro svolto nel suo complesso. Quando invece il contributo del singolo studente (inclusa la sua capacità di presentare il lavoro svolto), sulla base delle linee di indirizzo dei project work, sarà valutato negativamente, allora il punteggio assegnato dalla commissione a tale studente sarà proporzionalmente ribassato. Gli studenti possono in qualunque momento contattare i docenti per palesare criticità dovute a contributi insoddisfacenti di altri membri del gruppo o altre informazioni utili ad un'equilibrata valutazione. Un ribasso di 1 punto è ulteriormente possibile se il progetto nel suo complesso dovesse presentare criticità che non sono state già considerate nella valutazione dei singoli work package.

Consegna.

Entro il 14 giugno dovrà essere consegnato almeno il 50% nella seguente modalità: si richiede il 100% di WP1 ed una bozza principalmente di WP2 e addizionalmente di WP3 che corrisponda approssimativamente ad almeno il 50% del totale WP2+WP3. La consegna del 100% del project work sarà calendarizzata dal consiglio didattico (come specificato nelle linee di indirizzo), ed in mancanza di tali indicazioni, le scadenze entro cui consegnare saranno specificata dai docenti (sentiti gli studenti), una volta note le date degli appelli.

Validità della valutazione.

La valutazione ottenuta dura 12 mesi dalla consegna. In caso di mancato superamento dell'esame nei 12 mesi successivi alla consegna, lo studente può coordinarsi col docente per discutere la necessità di eventuali integrazioni al project work.

Sebbene preferibile che tutti gli studenti del gruppo partecipino insieme alla discussione e valutazione del loro project work; resta tuttavia possibile sostenere tale colloquio anche separatamente. Di norma, la discussione del project work a) precede di qualche giorno la prova teorica che vale 18 punti e che si tiene tipicamente nelle date degli appelli; b) avviene circa una settimana dopo la consegna del 100% del project work, per consentire ai docenti di consultare l'elaborato predisposto dagli studenti.

FAQ.

Q1: è impossibile evitare la coercizione se qualcuno mi forza a votare in sua presenza, giusto?

A1: una tipica nota mitigazione consiste nel consentire di rivotare annullando il voto precedente.

Q2: è ovvio che se c'è un virus nel mio computer allora il mio voto è insicuro, giusto?

A2: abbastanza vero ma nulla vieta di fare il boot con un sistema operativo su dispositivo read only

Q3: si può usare la blockchain?

A3: si può usare tutto; cmq cenni sulle blockchain saranno dati durante una lezione su tecniche per la decentralizzazione di metà maggio