PROJECT WORK – Algoritmi e Protocolli per la Sicurezza

L.M. Ingegneria Informatica

Docente: I. Visconti

A.A. 2022-2023

(versione del 09 Maggio 2023, integrazioni in rosso)

Premessa. Durante la pandemia (disclaimer: si tratta di scenari inventati) ....

Mister Joker, proprietario di un Sala Bingo decide di creare delle stanze virtuali online in cui le persone possono incontrarsi per partecipare a vari giochi di fortuna, ossia giochi dove sulla base di valori casuali c'è un vincitore (es., tombola, roulette). Mister Joker vuole spendere poco e quindi contatta un gruppo di studenti del corso di laurea magistrale in ingegneria informatica dell'università di Salerno chiedendogli di realizzare una funzionalità cruciale di tale software: "la generazione continua nel tempo di stringhe casuali"; tali stringhe devono essere quindi non controllate/decise/calcolate da nessuno (individualmente) dei partecipanti in una sala virtuale, ma comunque stabilita attraverso la partecipazione di tutti i partecipanti (e solo loro, ed il server visto che in molti giochi c'è la presenza attiva del Banco). Mister Joker vorrebbe una soluzione con massima trasparenza, altrimenti da casa tutti penserebbero ad imbrogli.

Chi è al potere ha da poco imposto il divieto di partecipare ad eventi sociali anche on-line a chi non possiede il Green Pass; quindi, chi lo possiede deve esibirlo per partecipare agli eventi sociali, e le stanze virtuali di una Sala Bingo sono considerate come appartenenti a tali categorie. Si è messo tra i piedi il garante per la protezione dei dati personali che ha imposto il divieto di invio su canali telematici del Green Pass in quanto esso mostra dati personali in eccesso rispetto a quanto strettamente necessario per l'accesso ai servizi. Il governo, quindi, ha deciso di pubblicare una call aperta a tutti per proposte di formato del Green Pass 2.0. Tale formato dovrà ancora prevedere la solita sequenza di informazioni del soggetto (cioè i dati già presenti nel tradizionale Green Pass) associate ad un'unica firma digitale rilasciata dall'autorità sanitaria. Tuttavia, oltre ad essere esibito di persona mostrando il QR-Code stampato, si richiede che chi lo possiede su smartphone/computer possa esibire telematicamente solo le informazioni strettamente necessarie sulla base del contesto (es., mostrare il tipo di vaccino, le date, o l'essere stati positivi al virus, insomma quello che serve anziché mostrare tutto), cioè, esibendo lo stretto necessario o per accedere ad un servizio. Gli studenti del corso di laurea magistrale in ingegneria informatica dell'università di Salerno, in cerca di pecunia sono intenzionati a partecipare alla competizione del Green Pass 2.0. Mister Joker vuole giocare d'anticipo e richiede quindi agli studenti di realizzare questa funzionalità per l'accesso alle sale virtuali della sua Sala Bingo, anche se ancora non sa quali specifiche informazioni tra quelle presenti nel Green Pass 2.0 dovranno essere esibite per accedere alla sala virtuale sotto la benedizione del DPA (cioè Data Protection Authority, cioè il garante). Tuttavia, questo non sarà un problema, perché gli studenti intendono progettare un sistema dinamico tale da permettere al proprietario del GP 2.0 di usarlo in sicurezza anche al variare delle politiche nel tempo circa quali dati bisogna possedere nel GP 2.0 per accedere ad un servizio. Inoltre, Mister Joker vuole che questo sistema sia anche utile per identificare le persone presenti nella sala virtuale, in modo che possano accedere al proprio conto virtuale da utilizzare per le vincite/perdite nei vari giochi. Gli studenti, quindi, progetteranno un GP 2.0 che 1) viene emesso dalla stessa autorità fidata "Ministero della Salute" che emetteva il GP 1.0; tale autorità

è fidata nello stabilire i dati anagrafici e sanitari similmente ad una certification authority che attesta i dati inseriti in un ceritficato digitale, per cui è coinvolgibile solo in fase di generazione di GP 2.0 (ed eventuali revoche), ma nulla di più; 2) permette ad un utente di identificarsi con la sala Bingo per accedere al proprio profilo, 3) permette successivamente ad un utente che ha un GP 2.0 che contiene informazioni che soddisfano la politica imposta dal garante, di accedere alla funzionalità di generazione continua di stringhe casuali.

Chiarimento: "per generazione continua" si intende che ogni volta che serve una stringa casuale le parti interessate a tale stringa (sarebbero i giocatori coinvolti nella partita) partecipano a generarne una. Ovviamente non può un'unica partecipazione essere tale da produrre tutte le stringhe che saranno usate in futuro senza ulteriori interazioni, in quanto ad esempio questo permetterebbe nei giochi di sapere quali saranno i prossimi numeri estratti o carte prese dal mazzo.

Nota: alcuni requisiti possono essere tra loro contrastanti e non è affatto chiaro che tutte le proprietà desiderate possano essere raggiunte in pieno. E' verosimile che tali sistemi si reggano su compromessi/assunzioni e vari meccanismi che provano a mitigare criticità sapendo che i rischi non sono evitabili in assoluto.

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, chi propone innovazione è di solito una volpe che vuole approfittarsi dell'ignoranza altrui. Sono i no-fox. Per evitare facili strumentalizzazioni da parte di tali complottisti è quindi necessario che un sistema 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 bontà limitando il danno che può essere causato da un qualunque avversario. Si tratta di una richiesta esplicita di Mister Joker che ha ricordato anche che la musica in background delle sue sale virtuali sarà di Franco Califano che diceva in una sua opera: "Non mi fido di nessuno".

Obiettivo del project work: individuare e realizzare le funzionalità richieste (cioè: generazione stringhe casuali, GP 2.0, identificazione al proprio profilo mediante GP 2.0) 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 benvenuta una

eventuale breve 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 utenti) e considerare che la correttezza del risultato è normalmente considerata prioritaria rispetto alla privacy (ma quando possibile vogliamo ottenere entrambe);

- 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 (o facilità) 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 rivoluzionari, ma solo che gli studenti usino adeguatamente le conoscenze acquisite durante il corso per esibire un ragionevole modello (cioè funzionalità con parti oneste + threat model + proprietà di resilienza), una dignitosa soluzione, una attenta analisi ed una appropriata implementazione.

Warning: il project work è un ulteriore momento formativo legato alle attività del corso, è naturale contattare i docenti per avere dei pareri ed in caso di pareri negativi non bisogna pensare negativamente sul punteggio (quello sarà stabilito solo sulla base della consegna finale e della presentazione) ma positivamente avendo avuto un'occasione per capirne di più.

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.

WP1: 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 model) 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: 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.

Evitare avversari (e definizioni) ridondanti, cioè che essendo descritti in modo diverso alla fine hanno lo stesso obiettivo e stesse risorse; considerare avversari (e definizioni) che sono strettamente più forti di altri avversari (e definizioni) soltanto se questo risulta cruciale nell'analisi della vostra progettazione (nel senso che si pensa di soddisfare una proprietà verso quello più debole ma non verso quello più forte, ceteris paribus).

WP2: Soluzione

Dato il modello identificato in WP1, mostrare un sistema 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 WP1. 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.

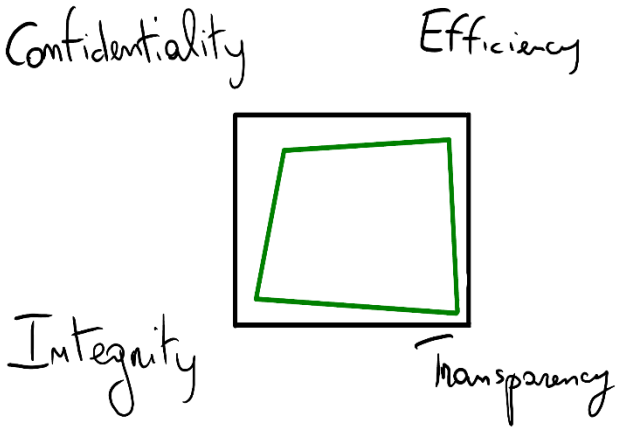
Nota 2.2: Si richiede l'uso corretto degli strumenti studiati durante il corso, non è necessario individuare/studiare nuovi strumenti, contattare la commissione in caso di incertezza.

Si consiglia di non risparmiare risorse sulla progettazione nel timore di dover implementare troppo in WP4. Nel caso ci sia un eccesso di contenuti da implementare è possibile contattare i docenti e definire un sottoinsieme di funzionalità da implementare in WP4. Warning: leggere attentamente la nota in WP4 che indica che è possibile progettare in modo da implementare tutto facilmente.

Se in WP2 si utilizza la tecnologia blockchain è importante specificare se "permissioned" o "permissionless", e nel caso "permissioned" è fondamentale individuare gli attori che ne avrebbero la governance e la visibilità dei suoi contenuti verso l'esterno.

WP3: 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 i sistemi progettati in WP2 (anche solo una parte di essi 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 un qualunque linguaggio quando è necessario programmare ed usare i comandi di OpenSSL per eseguire gli algoritmi che richiedono funzionalità crittografiche. Mostrare anche le prestazioni ottenute con la sperimentazione.

Se in WP2 si è deciso di utilizzare la tecnologia blockchain allora è possibile simularla in WP4 nel modo ritenuto più conveniente (es., un semplice file in cui si scrive in append e si legge).

Attenzione: questa traccia è stata pensata per essere risolta con una progettazione che può essere implementata utilizzando i comandi di OpenSSL e con elementare programmazione che formatta stringhe, invoca comandi, gestisce input/output. Non e' richiesto saper programmare usando librerie di crittografia (che del resto non sono state presentate durante il corso). Questo non è un corso di programmazione sicura.

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.

Il colloquio si svolge privatamente, per evitare che studenti che non consegnano il 100% entro la data prevista partecipino alle discussioni per "ispirarsi" ai loro colleghi.

Consegna.

La consegna consiste di un file pdf che illustrerà WP1, WP2, WP3 e le scelte implementative di WP4 insieme con eventuali analisi/discussioni. I sorgenti relativi a WP4 saranno invece allegati in un file di archivio. In tutto quindi la consegna consiste di 2 file.

Entro la fine del corso 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 può avvenire entro specifiche scadenze indicate dalla commissione in prossimità degli appelli.

La consegna del 100% dovrà indicare anche il "responsabile" per ogni WP. Si ricorda che in caso di gruppi di soli 3 studenti non ci sarà un responsabile per WP4. In caso di gruppi di 2 studenti allora la richiesta è che uno studente sia responsabile di WP1 e WP3 ed un altro studente sia responsabile di WP2 e WP4.

Il presente project work richiede un impego complessivo da parte dello studente di circa 50 ore, equivalenti a 2CFU di carico didattico. Il corso include esercitazioni e discussioni relate al project work per non meno di 16 ore. La valutazione terrà conto di questo carico atteso di lavoro in particolare concedendo ai gruppi costituiti da meno di 4 studenti una valutazione semplificata di WP3 e WP4.

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 con la commissione 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.

FAQ.

Q1: è ovvio che se c'è un virus nel mio computer allora non c'è sicurezza, giusto?

A1: abbastanza vero ma nulla vieta di fare il boot con un sistema operativo su dispositivo read only. Più in generale si può assumere che i dispositivi non siano corrotti.

Q2: si può usare la blockchain?

A2: si può usare tutto, è importante che lo si faccia con consapevolezza e che si chieda conferma alla commissione circa l'uso di strumenti non visti durante il corso.

Q3: ha senso considerare che una parte sia onesta nell'esecuzione del protocollo ma disonesta nel provare a carpire informazioni dai dati?

A3: si, ha senso almeno per 3 motivi. 1) perché una parte può essere inizialmente onesta e solo successivamente corrotta/attaccata; 2) perché la parte ha paura che il suo comportamento disonesto sia scoperto; 3) perché tale comportamento semi-onesto come indicato durante le lezioni può essere "forzato" dal protocollo mediante l'aggiunta di zero-knowledge proofs; è consentito l'utilizzo di tali strumenti purché sia ben definito il contesto in cui vengono utilizzati (cioè i claim che devono dimostrare devono essere chiari ed espliciti), e non sarà necessario entrare nel merito di come funzionano queste proofs e che prestazioni hanno (si può assumere O(1) anche se non è così). Tuttavia, bisogna evitare di usarle se non necessario in quanto gli strumenti visti in dettaglio durante il corso sono già adeguati per risolvere il problema.

Q4: in WP1 è meglio definire poche macro proprietà o tante micro proprietà?

A4: è meglio avere tante micro proprietà (ciascuna con un nome opportuno) in modo che poi è più limpido argomentare che la costruzione di WP2 ne soddisfi alcune e non soddisfi altre. Come detto in precedenza, evitare i casi di proprietà identiche o inutilmente identificabili come l'una più forte o più debole dell'altra (in particolare se poi la progettazione le soddisfa tutte).

Q5: può avere senso coinvolgere la giustizia?

A5: si, ma non come un irrealistico onnipresente osservatore di quello che accade. La giustizia dovrebbe intervenire solo su richiesta di fronte ad un'evidenza di brogli. Un attore malevolo teme di svolgere azioni disoneste se queste lasciano un'evidenza che può arrivare alla giustizia. In generale, tutte le risorse costose dovrebbero essere usate il meno possibile (es., non si può richiedere che quando uno entri in una Sala Bingo virtuale arrivi anche un carabiniere a casa a garantire che la persona non si stia coordinando con altri giocatori).

Q6: è possibile limitarsi ad avversari passivi?

A6: No, in WP1 vanno considerati tutti quelli che hanno senso, in WP3 l'analisi deve tenere conto anche degli attivi. Resta inteso che l'analisi degli avversari può far leva sulla possibilità che sia accertato

il comportamento disonesto il che tipicamente scoraggia la disonestà. Inoltre, si può far ricorso alle zero-knowledge proofs ricordando che: 1) non è necessario costruire tali proofs, basta assumere che esistano e che siano efficienti; 2) devono essere utilizzate solo dove strettamente necessario; 3) devono essere accuratamente specificati i claim che tali proofs intendono dimostrare.