Domande

Parte extra

Indice

Capitolo 1

Domande pacchetto 1 - AC

- Nell'ambito delle politiche basate sui ruoli, descrivere il principio di separazione dei privilegi (statico e dinamico) e fornire un esempio per entrambe le tipologie.
- Nell'ambito delle politiche discrezionarie, dire cosa rappresentano le ACL e le capability. Illustrare i vantaggi e gli svantaggi.
- Nell'ambito del modello relazionale multilivello, dire cosa si intende per tuple poliinstanziate ed elementi poliinstanziati e fornire un esempio per entrambi i concetti.
- Descrivere, tramite un esempio, perchè le politiche discrezionarie sono vulnerabili a Trojan horse.
- Nell'ambito del controllo dell'accesso, definire il concetto di gruppo e ruolo, evidenziando quali sono le differenze tra questi due concetti.
- Nell'ambito del modello di Biba, descrivere la politica low-water mark per oggetti. Questa politica garantisce l'integrità delle informazioni? Si richiede di giustificare la risposta.
- Definire il concetto di politica aperta e politica chiusa. Per quale ragione può essere utile definire un sistema basato sia su autorizzazioni positive sia su autorizzazioni negative? Quali problemi possono sorgere a causa della presenza di autorizzazioni positive e negative?
- Descrivere il concetto di poliinstanziazione. Fare un esempio di tabella con tuple e con elemento poliinstanziati.
- Nell'ambito del modello relazionale multilivello, dire cosa si intende per tuple poliinstanziate ed elementi poliinstanziati e fornire un esempio per entrambi i concetti. Si richiede di descrivere perchè nasce la poliinstanziazione e la differenza tra visibile ed invisibile.

- Descrivere cosa si intende per relation profile nel modello di autorizzazione che prevede tre livelli di visibilità (plaintext, encrypted, no visibility).
- Si richiede di fornire la definizione di politica di risoluzione dei conflitti "most specific takes precedence" e "most specific along a path takes precedence". Inoltre si richiede di fornire un esempio di gerarchia utenti-gruppi e di autorizzazioni in modo tale che l'utente alice possa leggere il file file1 quando si applica la politica "most specific takes precedence" per risolvere i conflitti mentre deve rimanere il conflitto quando si applica la politica "most specific along a path takes precedence" (usare una sola gerarchia utenti-gruppi per mostrare queste due situazioni).
- Nell'ambito del modello a matrice di accesso, si richiede di fornire la definizione di copy flag e di transfer-only flag. Fornire inoltre un esempio di comando per entrambi i flag e che riguardi il privilegio di scrittura.
- Cosa si intende per sistemi di controllo degli accessi aperti, chiusi ed ibridi?
- Nell'ambito dei modelli per la specifica di autorizzazioni basati su tre livellli di visibilità (plaintext, encrypted e no visibile), cosa cattura il profilo di una relazione? Quale è il profilo di una relazione R ottenuta tramite il prodotto cartesiano di due relazioni R_1 e R_1?
- Si richiede di descrivere le caratteristiche principali della politica per il controllo dell'accesso MAC (Mandatory Access Control).
- Nell'ambito delle politiche di controllo dell'accesso DAC, si richiede di descrivere le principali debolezze di queste politiche (trojan horse).

Capitolo 2

Domande pacchetto 2 - Query

- Nell'ambito delle tecniche usate per verificare l'integrità del risultato di query, dire quale è la differenza tra tecniche deterministice e tecniche probabilistice. Si richiede inoltre di fornire un esempio di query e come si può utilizzare una tecnica deterministica per verificarne il risultato della query di esempio.
- Nell'ambito delle tecniche per l'integrità del risultato di query, si richiede di descrivere l'approccio basato sul Merkle-tree e di fornire un semplice esempio di verifica, specificando la query, la tabella su cui viene eseguita eil Merkle tree costruito sulla tabell.
- Nell'ambito delle tecniche per la verifica della integrità del risultato di query, si richiede di descrivere le differenze principali tra le tecniche deterministiche e le tecniche probabilistiche. Si richiede inoltre di fare un esempio di tecnica probabilistica e del suo funzionamento.
- Nell'ambito delle tecniche usate per verificare l'integrità del risultato di query, dire quale è la differenza tra tecniche deterministiche e tecniche probabilistiche. Si richiede inoltre di fornire un esempio di query e come si usa una tecnica deterministica per verificarne il risultato.
- Nell'ambito delle problematiche di integrità del risultato di query, dire cosa si intende per correttezza, completezza e freschezza di una computazione.
- Nell'ambito del problema della integrit'a del risultato di query, dire cosa si intende per completezza, correttezza e freschezza del risultato di una query. Si richiede inoltre di descrivere una tecnica deterministica di controllo dell'integrità.

Capitolo 3

Domande pacchetto 3 - Query distribuite

- Nell'ambito di query distribuite, dire in che cosa consiste la tecnica per l'esecuzione di join detta sovereign join.
- Nell'ambito delle tecniche per l'esecuzione selettiva di query distribuite, descrivere cosa rappresenta il profilo di una relazione nel caso in cui si utilizzi il modello con tre livelli di visibilità (no visibility, plaintext visibility, encrypted visibility). Si richiede inoltre di mostrare un semplice esempio di query e autorizzazioni che richieda l'uso della crittazione per poter essere eseguita.
- Nell'ambito delle tecniche per l'esecuzione selettiva di query distribuite, l'approccio basato sulla definizione di viste si avvale di una riscrittura delle interrogazioni fatta in accordo al modello Truman oppure al modello non-Truman. Si richiede di descrivere questi due modelli e, in particolare, di fare un esempio di riscrittura basata sul modello Truman.
- Nell'ambito di query distribuite, quando due autorizzazioni definite come coppie [Attributi,Relazioni] possono essere combinate in modo safe? Si richiede di fornire un esempio.
- Si richiede di descrivere il concetto di profilo di una relazione nell'ambito del modello di controllo dell'accesso per query distribuite con uso di encryption. Inoltre si richiede di fare un esempio di interrogazione di join e di mostrare il profilo delle relazioni di partenza e della relazione che si ottiene tramite l'esecuzione della query.
- Nell'ambito dei modelli di autorizzazione per query distribuite che supportano la specifica del join path, dire cosa rappresenta il profilo di una relazione $[R_\pi,R_{\triangleright\triangleleft},R_\sigma]$ e fare un esempio di select-where query con associato il profilo relativo al risultato della query.

Capitolo 4

Domande pacchetto 4 - Differential privacy

- Dire formalmente quando un algoritmo (A) soddisfa la definizione di ϵ-differential privacy.
- Nell'ambito del concetto di differential privacy dire cosa si intende per global sensitivity e fornire un esempio.
- Nell'ambito della differential privacy, cosa si intende per global sensitivity? Si richiede di fare un esempio e di illustrare la relazione tra la global sensitivity ed il meccanismo di Laplace.
- Nell'ambito della differential privacy, si richiede di fornire la definizione formale di algoritmo che soddisfa la definizione di ϵ-differential privacy. Si richiede inoltre di descrivere, fornendo anche un esempio, cosa si intende per global sensitivity e a cosa serve.
- Dire formalmente quando un algoritmo (A) soddisfa la definizione di ϵ-differential privacy e spiegare la definizione.
- Nell'ambito della differential privacy, cosa si intende per composizione sequenziale e composizione parallela? Fornire un esempio.
- Nell'ambito della differential privacy, cosa indica il parametro ϵ?
- Nell'ambito della differential privacy, cosa si intende per modello interattivo e modello non interattivo?
- Quale è la differenza tra global differential privacy e local differential privacy?
- Cosa vuol dire che differential privacy è "chiusa rispetto a operazioni di post-processing"?

Capitolo 5

Domande che penso siano di altri pacchetti

- Nell'ambito delle blockchain, dire in cosa consiste la tecnica detta proof-of-work. E' corretto affermare che grazie a questa tecnica la scelta del nodo del sistema che crea un nuovo blocco è casuale?
- Nell'ambito delle tecniche per la specifica di preferenze utente per la selezione di cloud plan, descrivere i due tipi di preferenze (su valori e su attributi) che possono essere espressi e fare un esempio.
- Nell'ambito delle blockchain, si richiede di descrivere (ad alto livello) come funziona il protocollo del consenso.
- Nell'ambito delle blockchain, si richiede di descrivere la struttura di un blocco.
- Nell'ambito delle tecniche per la specifica di preferenze utente per la selezione di cloud plan, descrivere i due tipi di preferenze (su valori e su attributi) che possono essere espressi e fare un esempio.
- Nell'ambito delle blockchain, perchè è importante che ciascun blocco abbia nell'header l'hash del blocco precedente? Mostrare un esempio della sua utilità.
- Nell'ambito della specifica degli approcci per esprimere preferenze da parte degli utenti su proprietà dei cloud plan, si richiede di descrivere le tre techniche di ranking (pareto dominance, d-dominance, wd-dominance) e fare degli esempi per ognuna di esse.
- Nell'ambito delle tecniche per la specifica di requisiti utenti per la scelta di cloud provider, perchè è importante anche supportare, oltre che la specifica dei requisiti, anche la specifica di preferenze? Ad esempio, quali tipi di preferenze possono essere specificate?

Note:

- L'esame del 10/06/2024 è simile a quello che sarà il nostro
- L'esame del 3/07/2024 è simile a quello che sarà il nostro