ESAME - Sicurezza e Affidabilità

Fabio Ferrario
@fefabo

2023/2024

Indice

Capitolo 1

Crittografia

simmetrica vs asimmetrica Si spieghino le differenze tra crittografia simmetrica e assimmetrica

Risposta:

Simmetrica Nella crittografia simmetrica si utilizza una sola chiava, sia per cifrare che per decifrare un messaggio: Il mittente cifra il messaggio con la chiave k e lo invia al destinatario, che dovrà decifrare il messaggio con la stessa chiave k

Asimmetrica Nella crittografia asimmetrica ogni utente genera una coppia di chiavi (legate matematicamente), una pubblica e una privata. La chiave pubblica è accessibile in chiaro a tutti, quella privata invece rimane segreta e conosciuta solo a chi l'ha generata. Queste chiavi sono fatte in modo che se una viene utilizzata per cifrare un messaggio esso potrà essere decifrato solo con l'altra.
Quindi se devo inviare un messaggio a un destinatario lo cifrerò con la sua chiave pubblica, di modo che soltanto esso potrà decifrarlo con la sua chiave privata.

Si descriva la relazione fra numero di chiavi e utenti per la crittografia simmetrica e asimmetrica

Risposta:

simmetrica Per la crittografia simmetrica ogni coppia di utenti ha bisogno di una chiave segreta per potersi scambiare messagi, quindi il numero di chiavi necessario è $\frac{N(N-1)}{2}$

Asimmetrica Nella crittografia asimmetrica invece è solo necessaria una coppia di chiavi per ogni utente, quindi $2N$ chiavi.

Si spieghi il funzionamento della crittografia a **chiave pubblica**, indicando in particolare come si può usarla per implementare **firme digitali**

Risposta:

Crittografia a chiave pubblica Nei sistemi asimmetrici a chiave pubblica genero una coppia di chiavi, una pubblica e una privata.
Le due chiavi sono generate matematicamente in modo che un messaggio criptato con una chiave può essere decrpitato solo con la rispettiva altra chiave. Quindi se devo inviare un messaggio ad un altro utente, cripto il messaggio con la mia chiave privata e lo invio ad un altro utente che lo decripterà con la mia chiave pubblica (che è sempre disponibile).

Firme Digitali Per realizzare firme digitali, si crea un digest del messaggio tramite un algoritmo di Hashing e lo si critta con la chiave privata del mittente. Il messaggio viene quindi inviato al destinatario insieme al digest crittato, che verificherà la mia identità decrittando il digest con la mia chiave pubblica.
In questo modo avrà sia conferma che il mittente sono io, sia la conferma che il messaggio è integro verificando a sua volta con il digest del messaggio inviato.

2 Si descriva come si possono combinare crittografia a chiave asimmetrica e algoritmi di Message Digest per ottenere meccanismi efficienti di **firma digitale**

Risposta: Firmare un messaggio intero è computazionalmente molto costoso, quindi si effettua prima un digest (ad esempio con MD5) del messaggio e poi si usa RSA per crittare il digest.
Quindi i passaggi sono:

1. Il mittente crea il digest del messaggio da inviare.
2. Cifra poi il digest del messaggio con la sua chiave privata ottenendo così la firma digitale.
3. Infine invia il messaggio insieme alla firma.
4. Il destinatario, ricevuti il messaggio e la firma, decifra la firma con la chiave pubblica del mittente ottenendo così il messaggio e il relativo digest.
5. Per controllare l'autenticità del messaggio genera a sua volta un digest di esso e lo confronta con il digest ricevuto.

Capitolo 2

Sistemi Operativi

DAC-MAC Si descriva la differenza tra **DAC** e **MAC**, facendo un esempio di una politica di controllo degli accessi per ognuno dei due tipi

Risposta:

DAC - Discretionary Access Control il proprietario di una risorsa ne concede l'accesso ad altri utenti a sua discrezione.
Un esempio è google documenti, in cui il proprietario decide di dare accesso a una sua risorsa a un utente singolarmente.

MAC - Mandatory Access Control In questo caso il sistema impone un modello che limita e controlla la discrezionalità degli utenti nell'assegnare i diritti di accesso alle risorse.
Un esempio è la sicurezza multi-livello militare, in cui un utente può accedere soltanto a risorse che hanno un livello di segretezza uguale o inferiore al suo.

ACL Si descriva il funzionamento di una Access Control List

Risposta: Una Access Control List è una lista dove, data ogni risorsa, possiamo inserire chi ha diritto e che diritti ha (Lettura, scrittura, esecuzione). Una ACL ci permette di risparmiare spazio rispetta alla tabella completa, è facile determinare la lista degli utenti che hanno un diritto specifico su una risorsa condivisa ed è facile revocare/modificare l'accesso di un utente ad una risorsa.

Funzionamento Per una risorsa la ACL contiene una lista di utenti o di gruppi e i rispettivi diritti (ownership, read, write, execute).

ACL - Unix Si descriva il funzionamento di una Access Control List basata su 9bit come quella di Unix/Linux

Risposta: Unix utilizza un modello semplificato della ACL che utilizza solo 9 bit di protezione (per file). Vengono definiti i permesi soltanto per L'owner, un gruppo definito, e il resto del mondo. Per ognuno di essi abbiamo 3 bit (R,W,X) che definiscono i rispettivi permessi.

Questo tipo di ACL è molto più piccola ma permette una granularità molto inferiore.

Principi Si descrivano i concetti di Mediazione Completa e Principio dei Privilegi Minimi

Risposta:

Mediazione Completa Ogni tentativo di accesso deve essere controllato.

Bell-LaPadula Descrivere il modello Bell-LaPadula completo

Risposta: Il modello Bell-LaPadula è un modello MAC multilivello che nasce in ambito militare per garantire la confidenzialità dei dati. In questo tipo di modello gli utenti e le risorse sono classificati secondo dei livelli di sicurezza, in modo che un utente possa accedere ad un dato solo se il suo livello è maggiore o uguale a quello della risorsa.

Bell-LaPadula implementa due proprietà:

- No Read Up: Un soggetto non può leggere oggetti di livello più alto. (Simple Security)
- No Write Down: Un soggetto non può scrivere oggetti di livello più basso (impedendogli di trasferire documenti del suo livello a livelli più bassi). (Confinement)

Bell-Lapadula può essere esteso con **compartimenti**, in cui ad ogni risorsa e utente è assegnato un compartimento, e un utente può accedere ad una risorsa sse il suo livello è maggiore o uguale a quello della risorsa e se fanno parte dello stesso compartimento.

Autenticazione Challenge-Response