Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova del 14/6/2006

A. Si ha un sistema MAC per un sistema informativo di un'azienda, in cui si ha una classificazione in termini di livello secondo la scala U,C,S,TS (Unclassified, Classified, Secret e Top Secret) e in cui si individuano 3 categorie: Amministrazione, Vendita, Produzione.

   Si considerino entrambi gli approcci low-water mark per Biba, sui soggetti e sugli oggetti, e mostrare, per ciascuno di essi, quali operazioni della sequenza verranno rifiutate se comandate all'interno di una sessione da parte di un utente che gode della clearance (S,{Amministrazione,Vendita}) e per le operazioni accettate mostrare l'effetto dell'operazione sullo stato del sistema. Nel nome del file *file*_ X_ Y rappresentiamo con X il livello di sicurezza e con Y la categoria.

   1. read(file_C_A)
   2. write(file_C_P)
   3. write(file_S_AP)
   4. write(file_S_AV)
   5. write(file_TS_AP)
   6. write(file_U_DRA)

B. Illustrare le caratteristiche del modello di controllo dell'accesso "Chinese Wall".

C. Si supponga di avere un meccanismo di identificazione biometrica con un grado di precisione pari a 10^{-10} (che rappresenta la probabilità che, dati 2 membri scelti a caso della popolazione, l'identificatore biometrico dell'uno possa applicarsi all'altro).

   Si supponga quindi che l'identificatore sia utilizzato per svolgere indagini criminali. Supponendo che la percentuale della popolazione dedita ad atti criminosi è pari all'1% e che ciascun membro produce quindi un identificatore, quanto deve essere grande approssimativamente la popolazione per avere una probabilità del 50% di incolpare in almeno un caso un innocente?

   Illustrare quindi i contesti nei quali è interessante applicare strumenti di autenticazione di tipo biometrico.

D. Si discutano le tecniche di bit-commitment.

E. Si presenti e si discuta un'architettura di soluzioni di sicurezza informatica per la costruzione di un sistema in grado di gestire la verbalizzazione via Web degli esami universitari. Il sistema deve tenere conto delle esigenze di integrità e di riservatezza. Illustrare e valutare in termini di rapporto costi-benefici alcune alternative per l'autenticazione del docente responsabile di inserire i voti nel sistema.

F. Illustrare le criticità che caratterizzano la realizzazione di soluzioni PKI.