Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova del 14/6/2007

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 gli approcci sui soggetti high-water mark (per BLP) e low-water mark (per Biba). 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,Produzione}); 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. write(file_U_A)
   2. read(file_TS_A)
   3. write(file_S_P)
   4. read(file_C_A)
   5. write(file_U_A)

B. Illustrare le caratteristiche del modello di controllo dell'accesso basato sui ruoli. Discutere poi l'integrazione tra un modello basato sui ruoli e un modello MAC di tipo multilivello (BLP o Biba).

C. Le tecniche di autenticazione biometrica sono di norma efficaci se utilizzate in combinazione con altre tecniche. Se utilizzate da sole, richiedono di essere applicate in un contesto supervisionato. Discutere l'impatto di questo requisito.

D. Si discutano le tecniche crittografiche per il "secret sharing" (condivisione di segreti).

E. Descrivere le motivazioni per l'uso dei certificati, facendo specifico riferimento alla struttura dei certificati X.509. Mettere in evidenza anche i principali ostacoli allo sfruttamento delle potenzialità di questo strumento.

F. Illustrare le caratteristiche di base dell'algoritmo di cifratura Blowfish. Presentare possibili criteri da considerare per la scelta tra l'uso di 3DES o Blowfish in specifici ambiti applicativi.