Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova del 28/6/2007

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.

Mettere in evidenza e correggere sul vostro foglio le anomalie nell'etichettatura rispetto al modello di poliistanziazione a livello di tupla e a livello di elemento, mantenendo sempre costante l'etichettatura dell'attributo Città.

Nome	L_N	Stipendio	L_S	Città	L_C
Anna	U,{A}	2000	C,{A}	Torino	S,{P}
Anna	S,{A}	1000	U,{A}	Torino	U,{V}
Bruno	S,{PV}	2000	TS,{PV}	Roma	C,{P}
Bruno	TS,{APV}	3000	TS,{A}	Milano	TS,{A}

Dopo aver corretto le anomalie, mostrare nei due casi l'esito del seguente comando, eseguito da un utente con clearance S,{A}:

```
update Impiegati set Stipendio = 5000 where Nome = Bruno
```

B. Si ha un sistema che conserva le password di autenticazione nel modo corretto, ovvero con hash robusto combinato con un nonce (salt). Il sistema impone di cambiare la password con una periodicità prefissata. Illustrare in una sola frase la motivazione di questa politica. Mostrare quindi come il sistema può far fronte alle seguenti strategie elusive messe in atto dagli utenti.

1. L'utente riusa immediatamente la password precedente.
2. L'utente usa una password con una componente numerica e la incrementa ogni volta (es., GTaTr:w21 diventa GTaTr:w22).
3. L'utente usa due password e le alterna.
4. L'utente usa due password con una componente numerica; ogni volta che viene forzato a cambiare password usa l'altra password con il valore numerico successivo a quello precedentemente usato.

C. Illustrare il funzionamento della tecnica SKEY; mostrandone vantaggi e svantaggi rispetto all'uso nell'ambito di token di autenticazione.

D. Descrivere e discutere le proprietà di sicurezza forte e debole delle funzioni hash.

E. Descrivere la resistenza dei modi di cifratura ECB, CBC, CFB, OFB, CTR ad attacchi di sostituzione in cui l'avversario ignora la chiave ma conosce il testo in chiaro e può manipolare arbitrariamente i bit del messaggio (ad esempio, vuole variare l'ammontare monetario o la destinazione di un trasferimento bancario noto). Assumere, per le soluzioni che usano un Initialization Vector, che l'IV sia inviato in chiaro sul canale come prologo al messaggio cifrato.