

Sicurezza dei Sistemi Informatici

Prof. Stefano Paraboschi

Prova del 5/6/2014

- A. Confrontare il comportamento dal punto di vista della sicurezza delle soluzioni Random/Counter/SKey per l'autenticazione con token su canali monodirezionali.
- B. Facendo riferimento al contesto di un moderno sistema operativo per sistemi server, analizzare in modo sintetico l'impatto dell'applicazione di un modello MAC dinamico low-water mark, confrontando in particolare un approccio basato sui soggetti e uno basato sugli oggetti.
- C. Illustrare il principio di design che prescrive la definizione di un preciso "trust boundary" nella progettazione di applicazioni sicure.