Part Ib Introduction to Security

p3q4
RJA

Consider the following two separation-of-duty ~~policy~~ policies:

(1) A transaction needs approval from two ~~people~~, one in group A and one in group B

(2) A transaction needs approval from two distinct users of the system

Which of these is harder to implement using the standard Unix access control mechanisms, and why?

(10 marks)

Sketch an implementation of the easier ~~option~~ policy using Unix mechanisms.

(5 marks)

Describe at least two alternative mechanisms that might be used to implement the other policy.

(5 marks)

(A) (2) is harder because there's application state that can't be mapped on to Unix groups

Implement using sgid programs to move a transaction from (untrusted) to (Approved by A) or (Approved by B) then to (Approved by A and B)

Alternative implementations for the second policy include hardware tamper resistance, a trusted application and digital signatures.