Kieren Ng

Cybersecurity Homework 5

2/21/2018

1A. Yes

1B. No, the messages will be still encrypted so Eve will not understand.

2A. No, because the response requiring a calculation for the random value can’t be replayed, unless they get real lucky I guess.

2B. Yes, if Eve has ks she could hypothetically answer the question correctly.

3. No, because Eve couldn’t hypothetically come back with the same r3 as before, unless they get real lucky again.

4.8.

RBAC0- “contains the minimum functionality for an RBAC system” (Source: textbook pg 123)

RBAC1- “includes the RBAC0 functionality and adds role hierarchies which enable one role to inherit permissions from another role” (Source: textbook pg 123)

RBAC2- “includes RBAC0 and adds constraints, which restrict the ways in which the components of a RBAC system may be configured” (Source: textbook pg 123-124)

RBAC3- “contains the functionalilty of RBAC0, RBAC1, and RBAC2.” (Source: textbook 124)

4.8

a. For a DAC scheme, the number of relationships would be something like Ui\*Pi\*N, because there are Pi permissions per User, and there are N job positions with Ui users.

b. For RBAC there are roles, but there aren’t any variables for roles in the question so I’m going to add my own with R. N\* Ui \* R

4.12

There should be 3 roles for RBAC, one that can see R and below, and PG-13 and below, and G and below (if there are any below). As for permissions, it’s as it says above, you see can see the level and anything that’s lower.