ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2016

Homework 5

Hand out: Oct 27th, 2016

Due time: Nov 3rd, 2016 before 11:00 am

Question 1. The Bell-LaPadula model is used to enforce information confidentiality through controlling the data flow direction. In short, it can be summarized as “no read up, no write down”. To define the “up” and “down” in the system, the model introduces the relationship of “Domination” in security levels.

The security level (L1, C1) dominates the security level (L2, C2) if and only if L2 ≤ L1 and C2 ⊆ C1. Here L1 and L2 represent security clearance levels, and C1 and C2 represent subsets of categories to which the data belongs.

Assume that we have a system with four levels of security clearance: Top Secret (TS), Secret (S), Classified (C), and Unclassified (U), from high to low. The system also has three categories: Army, Navy, and Air Force. Please fill “dominate” or “not dominate” in the following blanks. (It reads as “the left side dominates (or not dominates) the right side”.)

(a) (Classified, {Army, Navy}) \_\_\_\_\_\_\_\_\_\_\_\_\_ (Unclassified, {})

(b) (Top Secret, {Army, Air}) \_\_\_\_\_\_\_\_\_\_\_\_\_ (Secret, {Army, Navy})

(c) (Secret, {Army, Navy, Air}) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Secret, {Air, Navy})

(d) (Secret, {Navy, Army}) \_\_\_\_\_\_\_\_\_\_\_\_\_ (Top Secret, {Army, Navy})

Question 2. The public key infrastructure (PKI) needs to handle the revocation of compromised keys. Currently, there are two basic approaches. The first one uses the certificate revocation list (CRL). The CRL is published periodically (for example, 8:00am every day). It contains the public key certificates that have been compromised. Another approach is to use Online Certificate Status Protocol (OCSP). Please study how OCSP works. Then write about 0.5 page to discuss the working procedure of OCSP, and the advantages and disadvantages of OCSP over the CRL.