ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2017

Homework 4

Hand out: Oct 24th, 2017

Due time: Nov 1st, 2017 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.

Question 3. There is a bank ***B*** that allows its customers to withdraw cash from their accounts at hundreds of specialized automated teller machines (ATMs) that are only for cash withdrawals (not for checking balances or performing other transactions). The ATMs operate in the following way. (In what follows E\_B () refers to encryption with the bank's secret key, in a symmetric cryptosystem.) The bank asks the customer ***C*** to select a secret number (called "personal identification number", denoted by PIN (***C***)). Then the bank issues the customer ***C*** a special magnetized card that contains the following two pieces of information (**on separate portions of the magnetized strip on the** **card**):

(1) The customer's account number at the bank (call it AcNr(***C***)).

(2) E\_B(PIN(***C***)).

Each ATM of that bank can perform E\_B (\*) computation, and also stores a list of all the valid account numbers. It does not store the dollar balance in each account (each ATM limits cash withdrawals to no more than $200 per day for each account, and each account contains at least $500 - the bank automatically closes an account whose balance falls below the $500 minimum).

When the customer ***C*** wants to withdraw cash from an ATM, ***C*** inserts the card and the ATM reads the information on it and then challenges ***C*** to enter PIN (***C***). The ATM then

(1) verifies that the AcN r(***C***) that it reads from the card is on its list of valid account numbers, and then

(2) encrypts (i.e., does E\_B(\*)) what ***C*** just entered and verifies that the result equals to the E\_B(PIN(***C***)) that is stored in the card.

If both (1) and (2) are successfully verified, the ATM allows the customer to withdraw the cash (subject to the constraint that the total amount withdrawn by ***C*** that day from that ATM does not exceed $200). The ATM also stores a record of the transaction that consists of the account number and the amount just withdrawn. At midnight every day, all the ATM machines communicate with the bank's main computer. The computer will update all the customer accounts by subtracting from their balances the amounts of cash withdrawn that day. This off-line operation of the ATM allows the customers to quickly withdraw cash even when the network is down or very slow (at peak-hours during the day); contrast this to an on-line operation, which would have required communication with the bank's main computer before a transaction can complete (and would have been problematic if the network was down or very slow at the time of the transaction).

Note that, if the card is stolen from the customer, the thief cannot obtain PIN(***C***) from the card because it is encrypted (this is why it is E\_B(PIN(***C***)) rather than PIN(***C***) that is stored on the magnetic strip of the card - **the latter would be insecure because the information on the** **magnetic strip of a card is easy to read and modify if you have the equipment**).

Please answer the following questions:

1. How can a dishonest customer ***M*** (who also has an account of Bank ***B*** and a Card from Bank ***B***) steal money from ***C*** (by withdrawing cash from the account of ***C***). Here we assume that ***M*** knows ***C***’s account number. He also has a machine that can modify information on the magnetic strip. However, ***M*** does not know the secret key of the Bank.