ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2018

Homework 3

Hand out: Oct 26th, 2018

Due time: Nov 2nd, 2018 11:59 pm

**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})

**Answer 1:**

(a) (Classified, {Army, Navy}) **Dominates** (Unclassified, {})

(b) (Top Secret, {Army, Air}) **Not Dominate** (Secret, {Army, Navy})

(c) (Secret, {Army, Navy, Air}) **Dominates** (Secret, {Air, Navy})

(d) (Secret, {Navy, Army}) **Not Dominate** (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.

**Answer 2:**

Prior to OCSP, Certificate Revocation List or CRL was the protocol for verifying certificate status. CRL protocol is still used by some servers today but it is a much more time-consuming process. CRL is a list containing the serial numbers of certificates that have been revoked. These lists need to be updated frequently by the issuer of the certificate. An outdated list is no longer reliable for identifying revoked certificates. Therefore, keeping the lists updated is tedious and due to the possibility, that revocation lists may not always be up-to-date, CRL process is often faulty.

On the other hand, Online certificate Status protocol (OCSP) is a simple request/response protocol which is used for obtaining online revocation information of certificates, from a trusted entity referred to as the OCSP responder. It performs a real-time lookup of a certificate revocation status. and OCSP requests don’t require the browser to check through long lists of revoked certificates to find certificate status. OCSP requests also contain less information than CRL requests and hence, can be processed much quicker.

**In a nutshell, here’s how OCSP works:**

**Step 1:** Web-server sends its certificate to the client.

**Step 2:** The client sends an OCSP request to the CA (OCSP responder) to find the revocation status of the received certificate.

**Step 3:** The OCSP responder uses the certificate serial number to check the status and responds with one of the three possible values:

a) **Good:** The "good" state indicates that the certificate is not revoked.

b)  **Revoked:** The "revoked" state indicates that the certificate has been revoked either permanently or temporarily. If the status of a given certificate is “revoked”, then the time that the revocation happened is indicated and optionally the reason for revocation might be included.

c)  **Unknown:** The "unknown" state indicates that the responder doesn't know about the certificate being requested.

**Step 4:** The CA responder keeps frequent updates with the CRL server to make sure that the list is current.

An OCSP request consists of a service request type, a protocol version number, one or more target certificate identifiers and optional extensions which may be processed by the OCSP Responder.

Responses consist of the version of the response syntax, name of the responder, responses for each of the certificates in a request, optional extensions, signature algorithm OID, and signature computed across hash of the response.

**Advantages of OCSP over CRL:**

* OCSP eliminates the need for clients to retrieve the CRLs (which could be very large sometimes) themselves. This facilitates less network traffic and better bandwidth management.
* Client-side complexity is saved as the clients don’t need to parse CRLs themselves.
* CRLs get bad public exposure because they may be seen as analogous to a credit card company's "bad customer list.
* OCSP may be used to satisfy some of the operational requirements of supplying more timely revocation information than is possible with CRLs.
* The OCSP responder can be reached anytime when the certificate has to be verified, whereas, CRL is vulnerable to attacks until the next update.

**Disadvantages:**

* The online mechanism of OCSP typically requires the relying party or the client is online whenever a question regarding the revocation status of a certificate is to be resolved. Therefore, a periodic publication mechanism would be better suited for offline operations, since in this case, the revocation information can be cached.
* The responses from an OCSP responder must be digitally signed, which may impact the performance. Additionally, in case of high traffic website, there may be overhead issues when OCSP requests are sent for every certificate.
* OCSP would only indicate if a given certificate has been revoked or not. It is not designed to verify if a certificate is within its validity period. OCSP does not ensure that the subject certificate is being used in proper context as might be indicated through the key usage and extended key usage or any policy qualifier extensions associated with the certificate. It is up to the relying party/client to perform those checks.
* An OCSP responder will only have knowledge of a few certificate authorities, therefore, OCSP would not be practical for validating certificates issued by multiple authorities. Furthermore, the relying party/client must know the proper OCSP responder to query--this information, like the CRL distribution points, can be included in the certificate, but often isn’t. Hence, the responder needs to know about the certificate in question and about the signing authority as well.
* In case the private key is compromised, there could be a possibility of man-in-the-middle attack, thus rendering OCSP unreliable. Furthermore, the messages are communicated over http, this isn’t a very secure method of communication.

**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. A customer has $550 in the account. Now he decides to withdraw a large amount of money (much larger than $550) from his account and then drive across border to country BBB overnight. How can he do that?
2. How can a dishonest customer ***M*** (who also has an account of Bank ***B*** and a Card from Bank ***B***) steal money from customer ***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.

**Answer:**

1. Since the bank will have multiple ATMs throughout the city, the customer could visit any one of the ATMs and enter his pin to withdraw $200. Since the ATM doesn’t store information regarding the balance, the customer could then visit other ATMs in the city before midnight and withdraw $200 from each ATM. This way, the customer could then drive across the border to country BBB, overnight, with an amount much larger than $550.
2. Customer M already has a card of his own and also knows the account number of customer C, so M could use the machine which can modify information on the magnetic strip, and change the account number in his card to that of customer C’s account number. Now M could go to any ATM, and when the ATM reads the card, it would think it belongs to a genuine customer C (because the account number has been modified) and when the ATM machine asks to enter the pin, M could enter his own pin, the ATM machine would encrypt this pin and compare it with the value on the card. It would result in a match and the ATM will hence dispense the cash from customer C’s account. In this way, a dishonest customer M can steal money from a customer C.