Sample Solutions and Comments for Quiz #2

Questions:

1. **(5 points)** Answer T(RUE) or F(ALSE) to each of the questions below.

[F]The AES cipher is not invertible.
[F]The Caesar's cipher is a poly-alphabetic permutation cipher.
[F]The CBC mode of operation is not recommended for the transmission of long messages.

[F]In ECB mode, the initialization vector IV is sent as the first block of the cipher-text.

[F]The length of the message block and key should be same when using AES.

2. (4 points) Which of the following (select all applicable) conditions a good public key cryptosystems has to meet?

A. It must be computationally easy to encipher or decipher a message given the appropriate key.
B. It must be computationally infeasible to derive the private key from the public key.
C. It must be computationally infeasible to determine the private key from a chosen plaintext attack.
D. It must be computationally infeasible to derive the public key from the private key.

Answers: _____A B C__________

3. (4 points) In a system that has 10,000 user accounts and is subject to off-line dictionary attacks, how much more time-consuming does salting make the job of attackers, who are aiming at finding a password for any account and use brute-force search? Be specific and explain your answer.

Salting makes the job of the attackers 10 000 x ✓ more time consuming because they have to redo each dictionary attack for every single account. ✓
Each guess from the dictionary attack must be combined with the salt of each individual account; thus, the attack is 10 000 x more time consuming

Contributed by Anish Mitra.

How does the situation change if the attackers are looking to find only password for one specific account, e.g., administrative. Be specific and explain your answer.

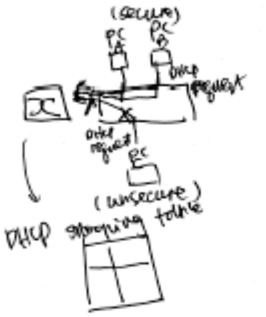
Then salting does not make the attack more time consuming. The salt value for each individual account is known; thus, the attacker can carry out the dictionary attack with the known salt value. An attack on a single account takes the same amount of time, regardless of whether or not salting is used

Contributed by Anish Mitra.

4. (8 points) You are a security analyst for a major bank. Your boss asked you to develop recommendations for countermeasures against the possible threat of denial of service attacks on the bank's DHCP service in the bank's intranet. Explain to your boss how such attack(s) work and sketch your idea of the countermeasure(s) you propose.

The attack would work because an attacker can pretend to be a certain user in the subnet and keep refreshing and requesting for DHCP address. The DHCP look-up table will quickly get filled up causing other users not able to get DHCP address. A DHCP denial of service can occur in this case.

port security & DHCP snooping can be used to prevent this type of threat.



Only ports that are marked secure are allowed for DHCP access. A DHCP snooping table with corresponding server information is built up for reference. If a port, say pcC is flooding the server with DHCP request, that port is marked as unsecure and is disallowed for future DHCP access.

Contributed by Jue Ni.

5. (4 points) Let us assume that you pre-registered for West Coast Security Forum (WCSF), which is an IT security professional conference held annually in Vancouver, and used your credit card to pay registration fees then. When you come to the forum first time, they find your name in the list of pre-paid attendees and give you your conference badge. You can now attend various WCSF with the badge. What type of access control structures are used in this example, ACLs and/or capability lists? Explain your answer.

- Registration of the conference —— ACL
  - the list of people (subjects) that have access to the conference (object) are attached to the object (or guards/people at the conference)
    hence this mechanism is ACL (

- Using the badge to go into various Conference — C-list (capability list)
  - the badge contains information associated with the users (subject) (ie the conference that the subject can attend and what right it has).
    ~~therefo~~ since this list is ~~associated~~ attached to the Subject,
    this mechanism would be C-List

Contributed by Vincy Tang.

Comments:

1. Question 3 asked the time difference of using **brute-force** to attack an off-line dictionary with and without salting. It is 10,000 times more time-consuming to attack a disctionary with salting.
   Salting would not increase the amount of work for attackers in the case of them attacking a specific account, including the administrative account.

2. Question 4 asked about the possible threat of **denial of service** attacks on the bank's **DHCP service**, some people were talking about other threats.

3. Question 5 involves both access control list and capability list.