Homework 3
Due: Monday, 11/28/2016 at 11:55pm PT
Solution: Will be posted on Wednesday, 11/30/2016

Full Name:
UCI ID Number:
Sources:

Guidelines:

• Use any word processor (or handwrite and scan your answers). Upload your solutions as a PDF to the associated EEE Dropbox (labeled “CS134: Homework 3”). No late submission will be accepted into the EEE Dropbox. The solution to the homework will be posted on Wednesday 11/30/2016, no late submission (even via email) will be accepted after posting of the solution.

• No collaboration is allowed. The only people you may ask for help are the TA and professor for the course.

• Copying, paraphrasing or copying answers from the internet or other sources is not allowed, and to do so would be a violation of academic honesty. You must list any sources you used to arrive at your answers (e.g., reference books, Wikipedia etc).

Warning: any submission not following the above guidelines may receive a score of zero.
1 [5 pts total] Multiple Choice Questions

There is only one correct answer for each of the following question. Answer justification is not required.

1. Which of the following is NOT an example of biometric authentication?
   A. Retina scans
   B. Handwriting pressure
   C. Voice recognition
   D. Kerberos
   E. All of the above

2. Which of the following can be used to avoid replay attacks in authentication protocols
   A. Nonce
   B. Monotonically increasing sequence number
   C. Time-stamp
   D. Random number used no more than once
   E. All of the above

3. What is a role of Key Distribution Center (KDC)?
   A. To establish a shared secret key between two parties
   B. To bind public key to a specific entity
   C. To securely relay a message from one side to the other
   D. To securely distribute shared public-/private key to multiple entities
   E. None of the above

4. What is a role of Certification Authorities (CA)?
   A. To establish a shared secret key between two parties
   B. To bind a public key to a specific entity
   C. To securely relay a message from one side to the other
   D. To securely distribute shared public-/private key to multiple entities
   E. None of the above

5. What protocol is Station-to-Station protocol based on?
   A. Lightweight Directory Access Protocol
   B. X.509 Authentication Protocol
   C. Fiat-Shamir Identification Protocol
   D. Diffie-Hellman Key Exchange
   E. None of the above

6. What is a typical lifetime of a certificate of root certification authorities?
   A. 24 hours
   B. 5-7 days
   C. 3-5 months
   D. 3-5 years
   E. All of the above
7. Which of the following is NOT true about X.509 Standard?
   A. It defines format for certificates
   B. It defines format for certificate revocation lists
   C. **It cannot be used in S/MIME, PEM, IPSec, SSL/TLS and SSH**
   D. It supports both hierarchical model and cross certificates
   E. None of the above

8. Which of the following is NOT an access right in Unix?
   A. Read
   B. Write
   C. **Delete**
   D. Execute
   E. None of the above

9. What is the length of proof when certificates are revoked, using certificate revocation lists (CRL)? Assume \( n \) is number of revoked certificates.
   A. \( O(1) \)
   B. \( O(log(n)) \)
   C. \( O(n) \)
   D. \( O(n^2) \)
   E. None of the above

10. Suppose Alice wants to encrypt and send a message to Bob. Which of the following should be included in the encrypted message so that Bob can detect the “freshness” of the message?
    A. Nonce
    B. Monotonically increasing number
    C. **Time-stamp**
    D. Her public key certificate
    E. None of the above
2  [5 pts total] Fill In The Blanks

1. The goal of Needham-Schroeder Protocol (Symmetric Key version) is
   to establish a session key between two parties.

2. The goal of Needham-Schroeder Protocol (Public Key version) is
   to perform mutual authentication.

3. Before using a certificate, one should check its expiration time and
   the most recent revocation status.

4. Certificate revocation tree (CRT) is based on Merkle hash trees.

5. Suppose a CRT contains two leaves: a hash of \((-\infty, 10)\) and a hash of \((10, \infty)\). If a certificate number 15 is revoked and needs to be added into that CRT, the leaves of the resulting CRT will become
   a hash of \((-\infty, 10)\), a hash of \((10, 15)\) and a hash of \((15, \infty)\).

6. An entity that can securely issue certificates is called Certification Authority.

7. The purpose of including a nonce in an authentication protocol is to prevent replay/playback attacks.

8. In X.500 naming, \(L\) stands for locality and \(O\) stands for organization.

9. In distributed settings, capabilities are the best access control type.

10. Some examples of objects in access control are files, memory and processes. An example of subjects in access control is users or processes.
3  [4 pts] Authentication

Recall the authentication protocol in Homework 1:

We learned from the solution of Homework 1 that an adversary can bypass this authentication protocol without knowing $K_{AB}$. This can be done by using a response from the second connection as a challenge reply to the first connection. This attack is called a “reflection” attack.

Present two ways to modify this authentication protocol in order to avoid the reflection attack. Write down the modified protocols in details and state your assumptions clearly.
Solution:

One way to do it is to change $K_{AB}(r_a)$ to $K_{AB}(r_a||B)$ and $K_{AB}(r_b)$ to $K_{AB}(r_b||A)$. The resulting protocol will be:

1. $A \to B$: $r_a$
2. $B \to A$: $K_{AB}(r_a||B)$
3. $B \to A$: $r_b$
4. $A \to B$: $K_{AB}(r_b||A)$

Or use distinct keys: $K_{AB}$ and $K_{BA}$ in different directions, i.e., changing $K_{AB}(r_b)$ to $K_{BA}(r_b)$. The resulting protocol will be:

1. $A \to B$: $r_a$
2. $B \to A$: $K_{AB}(r_a)$
3. $B \to A$: $r_b$
4. $A \to B$: $K_{BA}(r_b)$

Or use sequence numbers or timestamps instead of nonces in the above protocols.
4  [3 pts] Interleaving Attack

Consider the mutual authentication protocol with a pre-shared symmetric key $K$:

1. $A \to B : A, S$
2. $B \to A : E_K(S + 1, A)$
3. $A \to B : E_K(S + 2, B)$

Assume $E()$ is a secure block cipher (e.g., AES) and $S$ is a 32-bit monotonically increasing sequence number and maintained by both $A$ and $B$. $A$ and $B$ reject the authentication if $S$ in the first step is less than or equal to their maintained value.

Does the interleaving attack work on this protocol? If so, write down how the attack can be carried out and how to fix it. Otherwise, explain why the attack won’t work.

Solution:
Yes, the attack can be carried out as follows:

1. $E$ picks a very large number $S'$ (i.e. pick $S' = 2^{32} - 3$)
2. $E \to B : A, S'$
3. $B \to E : E_K(S' + 1, A)$
4. $E \to A : B, S' + 1$
5. $A \to E : E_K(S' + 2, B)$
6. $E \to B : E_K(S' + 2, B)$

One way to fix this is to make messages (2) and (3) asymmetrical. For example, (2) becomes $E_K(S + 1, B, A)$. 
Your website development company has 50 web developers and has developed over 10,000 web pages. A software developer may have one or more of the following access rights for a given web page: READ, MODIFY and KILL. READ allows viewing a page, MODIFY allows making changes to a page and KILL allows removing a page. If your goal is to minimize delay when a web developer tries to access a web page, which access control structure is the best: (1) Access Control Matrix, (2) Access Control Lists or (3) Capabilities? Justify your answer.

**Solution:** Since the number of objects is much higher than the number of subjects, we should use Access Control Lists. In the worst case scenario, using an ACL would take 50 iterations to search in a list. If we use capabilities-based access control, it would take at most 10,000 iterations since each capability contains at most 10,000 objects. Access control matrix is an abstraction of ACLs and Capabilities and should not be directly used.
6 [4 pts] Public Key Certification and Revocation

Alice and Bob communicated via signed email. Bob receives four messages from Alice: (1) one on Monday morning, (2) one on Tuesday night, (3) one on Wednesday night, (4) one on Thursday morning. Bob check all four emails on Friday at noon and find out that all signatures are valid. Consider two scenarios:

(a) How should Bob treat these messages from Alice if he found out that Alice’s public key certificate expires on Wednesday at 2pm.

(b) Suppose Bob receives her weekly CRL on Friday at noon, which includes Alice’s public key certificate. Alice’s public key certificate was compromised and she reported it on Wednesday at 2pm. How should Bob treat these messages from Alice in this case?

Solution:

(a) Bob should trust only first two messages since they were signed when Alice’s public certificate was still valid. Bob should reject messages (3) and (4) since Alice’s public key certificate already expired.

(b) Bob should reject all messages since Alice’s public key certificate has been revoked.
7 [4 pts] Public-Key Certificate

Look into the security settings for your web browser and answer the following questions:

(a) For your **personal** certificate, what signature algorithm is used?

(b) What is your public key length?

(c) If you inspect further in the security settings, you will see that your web browser installs many certificates of “root” (not intermediate) certification authorities (CA). Why does your web browser need to keep track of many root certificates, instead of just one?

(d) Take a look at one root certificate. What is its X.500 Distinguished Name? Also, answer (a) and (b) for this root certificate.

---

**Solution:**

(a) The answer can vary.

(b) The answer can vary.

(c) Because certificates of different websites may be signed by different CAs. So, we need to store many root certificates in order to validate certificates of various websites. Also, having only one CA could cause a single point of failure, which is a global damage, if an adversary can compromise that CA. With multiple root CAs, the damage from compromising one CA is localized within that CA.

(d) The answer can vary.
Suppose a certificate authority (CA) uses a Certificate Revocation Tree (CRT) to represent revoked certificates. The CA has issued a total of 500,000 certificates. Of those, 512 have been revoked.

(a) What is the height of the CRT?

(b) Suppose Alice wants to check whether Bob’s certificate is revoked or not. Using this CRT, how many hashes and/or signature verification does she need to compute?

(c) If another certificate is revoked, what needs to be updated in the original CRT to support this revocation?

(d) After you update the CRT in (c), what is the height of the new CRT?

Solution:

(a) 10. Note that 512 certificates are revoked but since we represent a leaf node as a range, we will need 513 leaf nodes for storing the corresponding ranges. Thus, the height of the tree is $\lceil \log(513) \rceil = 10$. (11 is also accepted if you start counting the height of the tree from 1.)

(b) She would need to re-compute the root hash and it would take as many hashes as the height of the tree (1 hash for the corresponding leaf node and 10 more hashes for hash values along the path to the root.). Then, she performs one signature verification on that root hash.

(c) One of its leaf nodes needs to be split into two new nodes. Suppose A is revoked and A is in (B, C), which is one of the leaf nodes. Then, (B, C) needs to be split into (B, A) and (A, C). Hashes of these two new nodes and their ancestors need to be computed. Signature for tree root needs to be re-computed as well.

(d) 10. (or 11 if the depth of the split leaf node is 10.)