Assignment 3: Exercises for Topic 3

Important Note. Due date: **July 13, 2020 (11:59am)**, the same due date as Assignment 4. The requested submission consists of the questions with * in the assignment, i.e., you need to submit Exercises 1, 4, and 5. In Exercise 8, (a), (b), and (d) are bonus questions for 1 mark.

Exercise 1*. In the public-key certificate system, suppose that the certificate authority (CA) employs DSS signature. Assume that CA's private key and public key pair is denoted by (sk_{CA}, pk_{CA}). Bob requests a public-key certificate for his key pair (sk_B, pk_B), which is a RSA key pair.

(a) Explain what Bob should submit to the CA to get the certificate for his public key pk_B.

(b) How does CA generate the certificate of Bob's public key? (You only need to specify the format of the certificate.)

(c) When Alice wishes to send some sensitive information to Bob using Bob's public key, what does she need to do before she performs the RSA encryption using Bob's public key?

(d) Why is a certificate authority necessary for a public-key system?

Exercise 2. Consider the man-in-the-middle attack when the Diffie-Hellman public keys are not signed in Protocol C.

(a) Explain how the man-in-the-middle attack works.

(b) Show how an attacker could impersonate the entities A and B by the man-in-the-middle attack.

(c) What are the secret keys that A and B, respectively, obtained by the end of the protocol?

Exercise 3. Assume that each of party A and party B has a pair of RSA public and private keys. The public keys are certified by a trusted third party. Try to design a key agreement protocol using public key for key transport and explain how mutual authentication is done (which is referred to as implicit authentication).

Exercise 4*. Security analysis on IKE Auth:

(a) Try to find a man-in-the-middle attack on the "IKE AUTH" exchange with the modification that the data fields over which the authentication payloads are generated such that $AUTH_i = Sig_{sk_i}(N_r)$ and $AUTH_r = Sig_{sk_r}(N_i)$, assume certificates are exchanged.

(b) Try to explore possibilities to conduct a dictionary attack in IKEv2, when the pre-shared secret S_{pre} is a password with binary length 8 bits. (Hint: A failed execution may expose a value $AUTH$ and the data it is protecting.)

Exercise 5*. Security analysis on TLS:

(a) Assume the key establishment algorithm is RSA, and the client authentication is not conducted, that is, message `CertificateVerify` is not sent. Try to identify an attack which hijacks the session by sending an attacker-generated "pre-master secret" to the server, where the messages $Finished$ can carry along without being detected by either the client or the server.

(b) Explain why the attack identified in (a) will not gain access to the server, if the client must enter a password before any further application data will be exchanged.

(c) Try to explain why key establishment algorithms RSA and DH cannot provide perfect forward secrecy.

Exercise 6. Consider the authentication vectors in AKA in 4G-TLE.

(a) Explain the functionalities of $f_i, i = 1, \cdots, 5$ used to generate the authentication vector in AKA, i.e.,

$$AV = (RAND, XRES, CK, IK, AUTN)$$

where

$$\begin{aligned} XRES &= f_2(K, RAND) \\ CK &= f_3(K, RAND) \\ IK &= f_4(K, RAND) \\ AK &= f_5(K, RAND) \end{aligned}$$

and

$$AUTN = (SQN \oplus AK)||AMF||MAC$$

where

$$MAC = f_1(K, RAND, SQN, AMF).$$

(b) Explain functionality of $SQN \oplus AK$. Which value is served as a masking value?

(c) Explain how the UE entity authentication and the network entity authentication are conducted.

Exercise 7. List the security flaws in WEP and comment that if you were a designer of WEP, you may argue how the design were considered as secure.

Exercise 8. A forgery attack on GHASH. GHASH is used in GCM in TLS and GCMP in WiFi, as well as EIA1 in 4G-LTE. In theory, it has been proved it is secure under the assumption that nonce cannot be reused. As you have seen, in the real world, in both 4G-LTE and WiFi, the nonce can be forced to repeat. Hence, an attacker is able to forge the authentication generated by GHASH. In the following, we will assume that a GHASH polynomial is evaluated in finite field $GF(2^4)$, defined by $t(x) = x^4 + x + 1$, a primitive polynomial, and α is a root of $t(x)$ in $GF(2^4)$. We give the following two pairs of plaintext and ciphertext.

plaintext	ciphertext
$M = 001100101111$	$C = 101000111001$
$M' = 100000110000$	$C' = 001011100101$

where the right most bit is LSB and each ciphtext is generated by a random cipher.

(a) ** Let $H = 0101$ in GCMP, compute $GHASH(C, H)$ and $GHASH(C', H)$. Find a ciphextext which has a valid hash value.

(b) ** In EIA1, let $P = 1111$, $Q = 0001$ and $OTP = 0011$ (i.e., without truncating), compute $GHASH(M, P)$, and $GHASH(M', P)$, the GHASH component in EIA1 for message M and M'.

(c) Provide an argument to show that a forgery for GCMP is successful even it is over the ciphertext.

(d) ** Show that after attacker intercepts the MAC-I(M) and MAC-I(M'), he can forge a valid MAC-I(M_{new}) where $M_{new} = 0110 \cdot (M + M') + M$. (Hint. Show that MAC-I(M_{new}) $= \alpha^5$[MAC-I(M) + MAC-I(M')] + MAC-I(M).)

(e) Identify a possible forgery when the attacker has only one MAC for both GCMP and EIA1.

Note. An example of the format for GHASH,

$$GHASH(M, H) = M_1H^3 + M_2H^2 + M_3H$$

where $M = (M_1, M_2, M_3)$ where

$$M_1 = 0011, M_2 = 0010, M_3 = 1111.$$

Exercise 9. Assume that a path consists of n nodes, $n > 2$. A piece of data D is transported from node 1 to node n.

(a) Assume that each node i, $i = 1, 2, \cdots, n$, has a pair of public and private keys (pk_i, sk_i) used for digital signatures, where the public key pk_i is certified by a CA, which is trusted by all the other nodes on the path. Can integrity protection and authenticity be applied on the path in both end-to-end and hop-by-hop manners through digital signature and how? (Hint: the data D can be protected by more than one signature.)

(b) If using symmetric key based message authentication code, what are the conditions about the shared keys among these nodes to achieve both end-to-end and hop-by-hop integrity protection and authenticity?