

## Solutions to Assignment 3

Xinxin Fan

### Solutions

1. (a) The long term authentication credentials for access authentication can be a public and private key pair, a symmetric key, or a password, which are stored in a well protected and secure authentication server.  
 (b) Since it is not quite expensive as before to build a rogue network in the era of pervasive computing, the first reason of conducting the mutual authentication is that an access node need to be sure that the network is indeed the one it wants to access instead of a fake one. Moreover, most access authentication methods also include a key establishment. Hence, implementing the mutual authentication is necessary to thwart a man-in-the-middle attack.  
 (c) It is assumed that a PoA is associated with an access server to conduct the access control through a trusted communication path in the sense that
  - the trusted communication are established through a cryptographic protocol; or
  - the path between the PoA and the access server is physically protected.
3. (a) Since  $RAND$  is given by the second state of the LFSR, we can obtain  $RAND = 1111$ . Therefore, we have

$$\begin{aligned}
 XRES &= f_2(K, RAND) = f(K \oplus 2, RAND) = f(1010 \oplus 1111) = f(5) = 1011, \\
 CK &= f_3(K, RAND) = f(K \oplus 3, RAND) = f(1011 \oplus 1111) = f(4) = 1101, \\
 IK &= f_4(K, RAND) = f(K \oplus 4, RAND) = f(1100 \oplus 1111) = f(3) = 1110, \\
 AK &= f_5(K, RAND) = f(K \oplus 5, RAND) = f(1101 \oplus 1111) = f(2) = 1001, \\
 MAC &= f_1(K, RAND, SQN, AMF) = f(K \oplus 1, X) \\
 &= f(1001 \oplus 1111 \oplus 0001 \oplus 0000) = f(7) = 0110, \\
 AUTN &= (SQN \oplus AK) \parallel AMF \parallel MAC = 0001 \parallel 0000 \parallel 0110.
 \end{aligned}$$

Finally, we can generate the authentication vector in AKA as follows:

$$\begin{aligned}
 AV &= (RAND, XRES, CK, IK, AUTN) \\
 &= (1111, 1011, 1101, 1110, 0001 \parallel 0000 \parallel 0110).
 \end{aligned}$$

- (b) The functionality of  $SQN \oplus AK$  is to protect  $SQN$  from eavesdropping by adversaries, where  $AK$  is served as a masking value.
5. (a) The VLR/SGSN first sends  $RAND_1 = 0001$  and  $AUTN_1 = 0111 \parallel 0000 \parallel 1101$  to USIM. After receiving  $RAND_1$  and  $AUTN_1$ , USIM does the following computations:

$$\begin{aligned}
 AK_1 &= f_5(K, RAND_1) = f(K \oplus 5, RAND_1) = f(1001 \oplus 0001) = f(8) = 1111, \\
 SQN_1 &= 0111 \oplus AK_1 = 0111 \oplus 1111 = 1000.
 \end{aligned}$$

Once USIM recovers  $SQN_1$  and checks the freshness of  $AUTN_1$ , it verifies  $AUTN_1$  as follows:

$$\begin{aligned} MAC'_1 &= f_1(K, RAND_1, SQN_1, AMF) = f(K \oplus 1, X) \\ &= f(1101 \oplus 0001 \oplus 1000 \oplus 0000) = f(4) = 1101 = MAC_1. \end{aligned}$$

Hence,  $AUTH_1$  is valid and USIM has authenticated the VLR/SGSN. The USIM then generates  $RES_1$  as follows:

$$RES_1 = f_2(K, RAND_1) = f(K \oplus 2, RAND_1) = f(1110 \oplus 0001) = f(15) = 1000.$$

The UE sends  $RES_1$  to the VLR/SGSN and it finds  $RES_1 = XRES_1 = 1000$ . Therefore, the VLR/SGSN has authenticated the USIM and the mutual authentication completes.

(b) After receiving  $RAND_2 = 0011$  and  $AUTN_2 = 0100$  from the VLR/SGSN, USIM does the following computations:

$$\begin{aligned} AK_2 &= f_5(K, RAND_2) = f(K \oplus 5, RAND_2) = f(1001 \oplus 0011) = f(10) = 1100, \\ SQN_2 &= 0100 \oplus AK_2 = 0100 \oplus 1100 = 1000. \end{aligned}$$

Then USIM verifies  $AUTN_2$  as follows:

$$\begin{aligned} MAC'_2 &= f_1(K, RAND_2, SQN_2, AMF) = f(K \oplus 1, X) \\ &= f(1101 \oplus 0011 \oplus 1000 \oplus 0000) = f(6) = 0111 \neq MAC_2 = 0011. \end{aligned}$$

Hence, the authentication fails in this case.

6. (a) The vulnerabilities of “attribute hiding” are as follows:

- If  $RA$  is generated using a weak pseudorandom generator, then an attacker can first guess  $RA$ .
- RADIUS implementations often only allow 16 character passwords and English dictionary words have very low entropy per character. Therefore, an attacker might launch an offline dictionary attack on the RADIUS shared secret  $S$ . Here a dictionary attack means that the attacker performs an exhaustive search from a pre-arranged list of values. When compared to a normal brute force attack, where a large key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed. This attack is usually applicable because system administrators tend to choose short and simple secrets.
- MD5 is designed as a hash function instead of a stream cipher encryption algorithm. Therefore, the probability that the dictionary attack is successful is much higher than any other password based encryption scheme where the encryption algorithm is implemented by a stream cipher.

(b) Note that in the Access-Request message the “Message-Authenticator” field is a 128-bit random string, which serves as a random challenge to the RADIUS server. Hence, if no “Message-Authenticator” attribute is included in Access-Request message, an attacker can impersonate the legitimate RADIUS server by replaying its response.

(c) As we have explained in (b), the “Message-Authenticator” in the Access-Request message is necessary for the NAS to authenticate the RADIUS server. Moreover, if the “Message-Authenticator” (i.e. the 128-bit random challenge) is not included, an attacker can replay the “User-Password” attribute to impersonate a legitimate NAS and the RADIUS server has no way to check whether Access-Request message comes from a legitimate NAS or a rogue one.