Computer and Network Security – Exercise no. 5

Submit in Pairs/Single to mailbox 19 by 1/2/12, 2:00 p.m.

1. Consider the IKE protocol shown in class.

   (a) We have seen in class how the CKY strings protect against DoS attacks in IKE main mode. Give a short explanation how the CKY strings mitigate the attack, and why the protection does not exist in IKE aggressive mode.

   (b) It was decided to change the computation of the CKY strings as follows. Assume that the server allows one IKE connection from a given IP at a given time. For any change to CKY_r explain whether there is still a protection against DoS for IKE in main mode (if there is an attack — show it, otherwise explain why it is secure):

   - $CKY_r = h(IP_i, IP_r, CKY_i)$,
   - $CKY_r = h(SA_i, IP_r, secret)$,
   - $CKY_r = h(IP_i, IP_r, rand)$,
   - $CKY_r = h(IP_i, SA_i, IP_r, secret)$,

   where IP_i is the initiator's IP address, IP_r is the responder's IP address, CKY_i is the cookie sent by the initiator, SA_i is the SA suggests by the initiator, *secret* is a 128-bit secret value known to the server only, and *rand* is a random string of 128 bits selected each time at random by the server.

   (c) It was suggested to alter the computation of $hash_i$ and $hash_r$ to be:

$$hash_i = PRF_{SKEYID}(N_i|N_r|CKY_i|CKY_r|SA_i|ID_i)$$

   and

$$hash_r = PRF_{SKEYID}(N_r|N_i|CKY_r|CKY_i|SA_i|ID_r)$$

   Additionally, the key derivation at the end of the first phase was changed to

$$SKEYID_d = PRF_{N_i|N_r}(g^{x_i x_r}|CKY_i|CKY_r|0);$$

$$SKEYID_a = PRF_{N_i|N_r}(SKEYID_d|g^{x_i x_r}|CKY_i|CKY_r|1);$$

$$SKEYID_e = PRF_{N_i|N_r}(SKEYID_a|g^{x_i x_r}|CKY_i|CKY_r|2);$$

   Is the new version of IKE as secure as the original version? If so, explain why or else, show an attack on the new version (that does not work on the original IKE). Distinguish between authentication with signatures and pre-shared-secret, and between main mode and aggressive mode.

2. Consider the SSL protocol shown in class.

   (a) SSL is widely used to secure communications of users with their banks. When a client wants to access his account, he connects to the bank's website using SSL. Most clients are individuals that do not hold any certificate, and in most cases, SSL is run without the CertRequest option. How the authentication of the user is done? If so, why to use SSL to begin with? Supply two reasons. (Answers longer than 6 lines will not be accepted).

   For the reminder of the question, a successful attack means that the adversary can successfully communicate with the other side, even after the SSL handshake is done. Moreover, the authentication of the users is done only by the protocol (no other authentication mechanisms are used).

   (b) Consider SSL with CertRequest. The Belgian secret service (BOB) uses a variant of the SSL protocol, called BOBL, which is a modified variant of SSL (with client authentication). BOBL mandates the use of CertRequest in the second message, but the computation of CertReply was changed to $CertVerify = Sig_{client}(Msg1, Msg2)$, where Sig is a secure signature algorithm. All certificates are signed by the CA run by BOB, and when the certificate is accepted by the BOB's servers it is verified to be issued by the BOB.

   Can James Bond impersonate a BOB agent when the communication is protected by BOBL? If so explain how he does so, else, explain why this is impossible.

   (c) In BOBL2 it was suggested to add a signature of the client on the pre_master_secret, i.e., $CertVerify$ is computed as: $CertVerify = Sig_{client}(Msg1, Msg2), Sig_{client}(pre\_master\_secret)$, where Sig is an RSA signature with no hashing (i.e., $Sig_{client}(x) = x^d \bmod n$ when (n, d) is the client's private key).

      i. Can James Bond impersonate a BOB agent?

      ii. Can James Bond impersonate a BOB server when communicating with a BOB agent?