CS 558 Introduction to Computer Security, Spring 2024

Written Homework Assignment 3

Solution

---

1. Change the symmetric key encryption into a hash function. Retain the identity within the hashed message and presume each party is aware of the other's identity.

2. (a): Includes Diffie-Hellman: $g^a \mod p, g^b \mod p$ in the messages. Or insert a separate session key into the encrypted messages.
(b): We can use timestamps to reduce the number of messages as shown in the course slides.

3. (a): Before authentication, Bob needs to possess Alice's password, likely acquired when Alice registers herself with Bob.
(b): Focus on the pro and cons of using password.
Advantage: cost free, convenient to use, easy to change...
Disadvantages: password is easy to guess, and other password cracking issues we discussed in class.

4. We can change the 4th message to, say, $[\text{h(msgs, SRVR, } R_A, R_B, \text{ S)}]_{Bob}$. We change the 4th message since in the original protocol this is where Alice authenticate Bob based on Bob can use his private key to retrieve the S, which can be used to derive K.
In the changed message, R_A,R_B and other messages could be optional. And S can be replaced by K. But the main point is this reply has to be signed by Bob, and message contains S or K, as well as hashed value.

5. a. Phase 1 is analogs to SSL session, which does the mutual authentication and establishes a key. Phase 2 is analogs to SSL connection, which establishes the actual IPSec connection.
b. In symmetric key mode, we have shown the dilemma in class that receiver need the other party's identity to retrieve the information but identity is encrypted. And the solution is to use IP address as ID which violates one of the goal of main mode that is to hide the identity. On the other hand, the public key mode can hide the identity.
