Information Systems Security
Series 7 Correction - Authentication and Key Establishment Protocols

December 8th, 2021

Exercise 1 : Trying a Basic Authentication Scheme

C can initiate two instances of the protocol, one with A, one with B, and authenticate as A to B as follows :

- C sends r_1 to B,
- B sends $(r_2, K^b_{priv}(r_1))$ to C,
- C then starts the protocol with A, and sends r_2 as the challenge.
- A then sends back $(r_3, K^a_{priv}(r_2))$ to C,
- And C can just send the $K^a_{priv}(r_2)$ he just received to B. Then B accepts "A"'s identity, and C has authenticated as A.

Exercise 2 : Improvement of the Authentication Scheme

We can't apply the same method, but if A starts the protocol to authenticate to C, then C can use that to authenticate as A to B :

- A sends r_1 to C,
- C sends the same r_1 to B,
- B sends back $(r_2, K^b_{priv}(r_1 \parallel r_2))$ to C,
- C then answers to A, and sends $(r_2, K^c_{priv}(r_1 \parallel r_2))$,
- A sends back $K^a_{priv}(r_1 \parallel r_2)$ to C,
- But then, C can just send the received $K^a_{priv}(r_1 \parallel r_2)$ to B, and thus manages to authenticate as A to B.

Exercise 3 : Diffie-Hellman

We consider that p and α were sent to both Alice and Bob before the beginning (if Alice generated p and α, then she sends both to B at the same time she sends $\alpha^x mod p$).

- Alice computes $\alpha^x \mod p = 3^7 \mod 17 = 11$ and sends 11 to Bob.

  Bob computes $\alpha^y \mod p = 3^{11} \mod 17 = 7$ and sends 7 to Alice.

  Alice computes the key $K = (\alpha^y)^x \mod p = 7^7 \mod 17 = 12$.

  Bob computes the key $K = (\alpha^x)^y \mod p = 11^{11} \mod 17 = 12$.

  Alice and Bob both have the shared secret key, K = 12.

- Charlie chooses $x' = 3$ and $y' = 5$.

  Charlie intercepts Alice message ($\alpha^x \mod p = 11$), and answers with $\alpha^{y'} \mod p = 3^5 \mod 17 = 5$.
  Alice computes the key $K_{AC} = (\alpha^{y'})^x \mod p = 5^7 \mod 17 = 10$.
  Charlie computes the same key $K_{AC} = (\alpha^x)^{y'} \mod p = 11^5 \mod 17 = 10$.

  Similarly, Charlie intercepts Bob's message ($\alpha^y \mod p = 7$), and answers with $\alpha^{x'} \mod p = 3^3 \mod 17 = 10$.
  Bob then computes $K_{BC} = (\alpha^{x'})^y = 10^{11} \mod 17 = 3$.
  And Charlie computes the same key $K_{BC} = (\alpha^y)^{x'} = 7^3 \mod 17 = 3$.

  And now Charlie has two keys, one to communicate with Alice, the other with Bob. And Charlie can now intercept all messages between Alice and Bob, decrypt with one key, read or change their content, and then encrypt with the other key and sending it to the intended receiver. Charlie has a total control over these messages, and Alice and Bob don't even know that Charlie is involved.

Exercise 4 : Simple Key Establishment Protocol Analysis

This protocol only respects Implicit Key Authentication :

- We have Implicit key authentication : only A and B can compute the session key, as the secret long-term key S is needed.

- We don't have Key confirmation, since A and B do not proove to the other that they have the key. (We don't know if they have received the random number sent by the other).
- We don't have Perfect forward secrecy : an adversary that read and saved each exchange can compute all past session keys when he gets the long-term key S.
- And we don't have Future secrecy : A passive adversary having compromised the secret long-term key US can just read the random numbers and build each new session key without needing an active attack.