CS528 Assignment II

Luke Jiang, jiang700@purdue.edu

February 2022

1 Question 1

- for key length of 80: $\frac{2^{80}\ (keys)}{2^{60}\ (keys/sec)} = 2^{20}\ sec = \frac{2^{20}}{24*60*60}\ days \approx 12\ days$
- for key length of 128: $\frac{2^{128}\ (keys)}{2^{60}\ (keys/sec)} = 2^{68}\ sec = \frac{2^{68}}{24*60*60*365}\ years \approx 10 * 10^{12}\ years$

2 Question 2

- The missed security principle is the principle of least privilege. Accessing SSH version should be a privileged operation and unverified clients should not have such privilege.
- The missed security principle is the principle of complete mediation. The servers' privileges are cached and not authenticated upon each access.

3 Question 3

- a) Second Preimage Resistant: Since the solution contains only one answer to be encrypted, Alice only needs to make sure that it's infeasible for Bob to come up with a different solution whose hashed value collides with Alice's hashed solution.
- b) Preimage Resistant: Since the hash value is read-only, an attacker must make sure that the modified binary files produce the same hash value. Otherwise, the modifications will be detected by the system.

4 Question 4

- a) An attacker may send a package containing a very long `prev_end` field, which causes content of the subsequent packages (whose `fp->offset` is smaller than `prev_end`) discarded by the program.
- b) We can replace the old data with the new data after alignment.

5 Question 5

- a) Yes, it can. The adversary can fill the third block, which is within the comment field, with desired header plaintext and use the produced cyphertext directly as the header of the attacking package.
- b) No.

6 Question 6

- a) Yes. since the recipient, the message and the nonce are all signed by A, B can ensure that A is sending the message to it with message m.
- b) No. An attacker can intercept A's reply, modify the message and send the tampered message to B.
- c) No. An attacker can intercept A's reply, replace the original encoded message with a tampered message encoded using B's public key and send it to B.
- d) No. An attacker can intercept A's reply, decode the message and nonce with the B's public key, replace the message and encode with B's public key again before sending it to B.
- e) Yes. Even though the recipient is not included in the message, B can still verify that the message is meant to be sent to it because the nonce is signed by A.