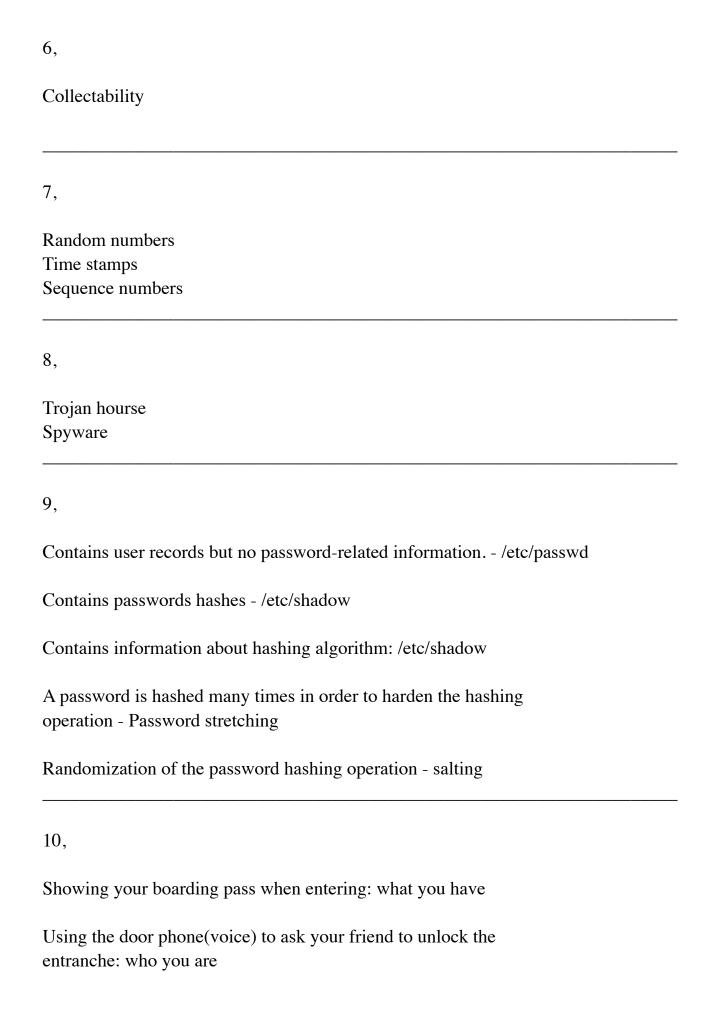
Computer Security - IV10113 Quiz 2

1,
True
2,
False
3,
False
4,
True
5,
-Nonces help to protect against playback(replay) attacks The nonce is already used and cant be reused, next nonce is what I get from reciever.
-Nonces help to protect from attacks where an imposter claims to be Alice and reuses previous information to prove it.
-Bob generates a nonce and challenges Alice to encrypt it. If Alice can encrypt the nonce, Bob knows that she has the key, and she has been authenticated



Signing a contract by putting your name in handwriting on paper: what you have

unlocking a door by entering a passcode: what you know

11,

Prevent the use of dictionary words in password

Use a slower function for computing password hash

Blocking an account after too many unsuccessful login attempts

12,

Buffer overflows are possible because of mistakes or oversights by the programmer.

With a properly designed buffer overflow attack, the attacker may take control over the program being attacked.

13,

The salt is generated by the server

The salt makes offline dictionary attacks more difficult

The hash is computed from the salt and Alice's password