Casper Kristiansson 2022-11-25

Homework 4

Question 1

A)

A main advantage of using timestamp compared to nonces is that it is less expensive. Timestamp works nearly identical to nonce beside that it is much more cost efficient because it can be derived from the current information rather then a random number generator for example.

Another main advantage of using timestamps is that it can prevent replay attacks from happening. Replay attacks happen when an intruder knows what information has been passed between the two people communicating. Using the information, the attacker can pose as another person. By using a timestamp, we can make sure that the two participants must perform something within the clock skew. Before the period is over there is still time for a replay attack to happen if the attacker finds out the session key. But in general, this becomes hard because the clock skew period can be modified by the users.

B)

Because the timestamp and session key are encrypted separately an attacker could use the information sent to decrypt the timestamp T. By doing this the attack can set its own value of the timestamp which means that the attacker doesn't have to act within the time screw. This means that by just sending the encrypted session key and the new timestamp the attacker can figure out the session key after the receiver responds.

Question 2

A)

The two constant strings **CLNT** and **SRVR** are used as certificates so that both the client and the server can identify themselves, when they are sent, they are being encrypted. This is to protect against reflection attacks.

B)

In the given scenario Alice will authenticate Bob. This is because we want to encrypt the messages sent from Alice and make sure that they do not end up in the hands of the wrong person.

C)

No, Bob does not need to authenticate Alice. This is because using SSL protocol the server doesn't authenticate the client because it is not. While for example, other protocols like TLS both the client and the server authenticate each other.

Question 3

A)

Question 4

A)

Proof-of-work (PoW) in the blockchain is the process of a user/machine proving that they have performed a certain type of work. The reason why it is also needed is to make sure that only valid blocks are added to the network, and for example not revalidating the same block multiple times. The responsible person to solve PoW is the miner when a new block is added.

B)

Proof-of-stake like proof-of-work is responsible for creating new blocks in the blockchain. But unlike PoW where the miners perform cryptographic tasks, PoS miners hold and stake tokens. Proof-of-stake also uses a random validator for creating new blocks and validating transactions. The advantage of doing this is that it becomes less risky if an attack on the network would happen (for example with the 51% attack). This means that PoS wants to have a decentralized blockchain while PoW uses a centralized blockchain for mining.

C)

The key takeaway from Proof of Elapsed Time where each node gets a random wait time which it must wait for. The miner with the shortest time wins the block in each iteration. Doing this allows a much more fair lottery system for which node gets the next block. This kind of system is like Proof-of-work while a key difference is that it consumes less power and resources. This is because when a node is sleeping it is allowed to switch and perform other tasks.

Question 5

A)

Transaction-Ordering-dependence (TOD) builds on the principle, as an example, that if a user wants to buy something at a certain price an attacker could adjust the price that the user is paying. Meaning that the user will pay more. This happens because while a purchase is being processed the attacker can adjust the price before it executes which will result in a more expensive price.

In the Raffle example, if the user calls the method $process()$ the attacker could then also call $process()$ with the same value. If done correctly the attacker could set the current reserved[value] to something else besides 0 which will lead to the original user will not be able to reserve a number and the attacker receiving the reward instead of the given user.

B)

The reason for using a random number generator is to protect against attackers. As we know timestamp is not a good way for protecting against attackers because it is vulnerable to miners that might change it. Therefore, the suggested algorithm for finding a random number by both using a seed and a password protects it against attackers. Attackers want to try to find how the numbers are generated but because it is combined with a string/password that cannot be guessed it would become an impossible task.

Question 6

A)

There are multiple ways an attacker could make use of poisoning attacks in machine learning. An example of this is by manipulating the input data for a machine learning model so that the predictions that it makes becomes useless. Meaning that the model will start to make bad predictions and stop working. An attacker's objective for doing so could be to mess up the reliability of the machine learning model, this becomes a big problem if the model is developed for commercial services.

B)

Yes, poisoning attacks can be detected. Usually, when an attacker performs a poisoning attack, they will poison the d_{train} dataset. This means that if we use the d_{test} data set and the model we can make sure that the predictions that model G is making are correct by comparing it to the d_{test} data set. If the model is making the wrong prediction against the d_{test} dataset we know that a poisoning attack could have happened.

C)

As we know there are multiple ways for an attacker to perform an attack on a machine-learning model, data poisoning, evasion, and model extraction. Especially today when machine learning is being used more and more it's becoming important to protect against these types of attacks. A couple of different ways of protecting against these would be backdoor detection, training data sanitization, and model/algorithm protection.