CS 203 / NetSyS 240 Spring'25 – FINAL EXAM: Sample Problems

Problem

A) How does DNS cache poisoning attack work in general (answer in 3-4 sentences please)?
B) What is the role of TXID in DNS query replies?
C) How long (in bits) is TXID? Would doubling its length be useful? Why?

Problem

Recall the Dining Cryptographers problem setting with 3 diners. From the point of the view of the **non-payer**, answer the following:
A) What happens if all three declare "SAME" at the end of the protocol.
B) What happens if one says "SAME" and two say "DIFFERENT"?

Problem

How does a merchant (Bob) use the Tor anonymity network to set up a location-hidden service? How does a customer (Alice) learn about Bob's location-hidden service and how does she use it? Carefully list all necessary steps.

Problem

Recall TCP SYN flooding attack and countermeasures. The server computes a SYN cookie as:

F (source-addr, source-port, dest-addr, dest-port, coarse-time, server-key)

A) Can ***F()*** be a public key encryption function, i.e., server-key = server's public key? Explain.
B) Why does the server include a timestamp in the cookie? What would happen without it?

Problem

Recall the SYN Flooding attack and the cookie-based countermeasure discussed in class. Suppose that we modify the latter so that, instead of using symmetric encryption (or HMAC) to generate a cookie, the server signs (using its private key) the IP source address, port #, coarse time etc., of the incoming TCP SYN packet, and the resulting signature is the cookie subsequently returned to the client (SYN-ACK). That way, the client can verify that signature and make sure that it's talking to the right server. Also, the server would be able to check its own signature when the cookie is returned by the client in the 3rd message of the TCP handshake (ACK). How cool is that? If you like this method, explain why. If you don't like it, identify its drawbacks.

Problem

Suppose Alice and Bob each have a TOR Hidden Service: THS-Alice and THS-Bob. Alice lives in a place where alcohol is taboo and Bob lives in a place where humor is forbidden. Alice sells cocktail recipes, and Bob sells funny (but sometimes offensive) cartoons. (Note that both types of "goods" are digital.) Design a scheme so that Alice and Bob could perform *barter* using their respective Tor Hidden Services, i.e., instead of paying each other in some form of currency (money), Alice would "exchange" one cocktail recipe for one of Bob's cartoons. Try to make your protocol as fair as possible. Can it ever be perfectly fair? "Perfectly fair" means that – if the protocol breaks down at some point, or one of them aborts – neither party has any advantage over the other.

Problem

Suppose that, starting today, UCI is blocking all packets to/from your favorite streaming service using a firewall that works by checking source and destination IP addresses and discarding packets if either the source (of incoming) or destination (of outgoing) packets are in that streaming service.

To survive for the remainder of the quarter, you must find a way to bypass this restriction. Explain how IPSec can help you to bypass the firewall and regain access to your favorite streaming services. Which IPSec mode (Tunnel or Transport) is more appropriate considering this goal and why?