Program Model (TorForum)

We will provide a library with an API that allows a client to post anonymously to a central forum. When a client calls a method such as postMessage() from the library, the message will be onion routed and sent to the forum server and the forum server will return a message to the client acknowledging the request. In our demo, we would to have 6-10 onion routers running on individual VMs, one VM for the forums server, and one VM for the directory server. We will run multiple clients on other VMs that make API calls to post messages to the forum. We will show that the messages is relayed through the onion routers and reaches the forum, and the forum can send something back through the same relay network to the client that sent the request. We will also disconnect one of the nodes in a known relay circuit, and show that the message will now be sent through a new relay.

Forum Application

- There will be a forum hosted on a separate server
- A client that wants to anonymously post on the forum will use the Onion Proxy to send a message to the TOR network which will eventually reach the forum

Node Types:

- Directory server which knows the location of all the Onion Routers
- Onion Router Nodes
- Client (Onion Proxy)

Topology:

- Star topology between directory server and Onion Routers
    - Onion Routers send heartbeats to the server to detect disconnections (this is only for the purpose of sending Onion Proxies an updated list of connected Onion Routers)
- Onion Routers will not be connected to each other until an Onion Proxy forms a circuit in which the participating Onion Routers will send messages between each other

Typical Onion Routing Protocol:

- Server has a list of all nodes and their corresponding public key in the TOR network
    - Onion Routers register and share their public key with the server to join the network
- Set up TOR network:
    - Client (Onion Proxy) connects to a directory server and ask a server for all onion routers (OR/node) (or a random subset of nodes)
    - Pick at random an entry guard, relay node(s), and an exit node
    - Establish shared keys between client and each OR via Diffie-Hellman key exchange
        - We will do this incrementally at each node: i.e. the client will establish and shared key with the guard node by talking to the guard node directly; then the client will establish a different shared key with the next node in the circuit by tunneling through the guard node; this will repeat until the exit node.
    - Create asymmetric encryption keys from shared keys and use them to encrypt/decrypt client's message
        - Forward order:
            - client encrypts message with the guard node's shared key -> relay nodes' shared keys -> exit node's shared key
            - When the corresponding nodes receive the message, they decrypt it with the shared key they have with the client

        - Reverse order: nodes on the way back to the client will each encrypt the message with the shared key it has with the client.
- TOR network:
    - Whenever a node receives a message, it decrypts the message with the private key
    - This reveals the next hop's IP
    - Send the message further to this IP

Threat Model

- How to prevent against people sniffing at the exit node
    - All clients of this system will have the public key of the forum server, each message sent by the client will encrypted using the public key of server so that exit node can not determine the message and identity of the sender
- How to prevent traffic analysis attack
    - Based on message size
        - Make each message a fixed size
    - Based on timing of sent messages
        - Randomize a delay
- Disconnections
    - Nodes will wait for ACK back from node it transmitted a message to.
    - There will be a timeout time for how long a node should wait for a timeout
        - Account for different node speeds?
    - When an ACK is not received, it will propagate a disconnected error back to the client.
    - Not sure about detecting a disconnected error when waiting for a message back from the destination (forum)... ?
- Other threats…..