CS-523 Advanced topics on
Privacy Enhancing Technologies

Anonymous Communications
Live exercises

Carmela Troncoso
SPRING Lab
carmela.troncoso@epfl.ch

You decide to contribute to the Tor network by buying two servers and setting them up as onion entrance and exit nodes. You need to place these routers somewhere.

Discuss if there is a change in the anonymity (and against which adversary) if you place the nodes:

a) in your house
b) in different areas in your country
c) in different countries.

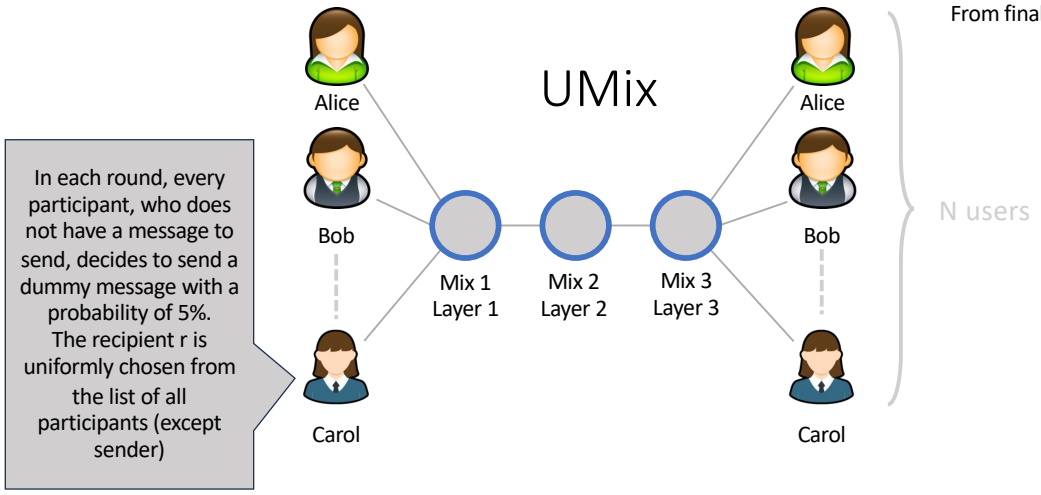
If an adversary doesn't have the capability to observe both ends of a Tor circuit, addition of nodes (and where they are placed) does not change the anonymity benefit. However, diversity in node placement can affect anonymity in the following ways:

- If the nodes are in your house, they could provide an advantage to an adversary such as your ISP or other local eavesdropper, if the client happens to use both entry and exit nodes.
- If the nodes are in different areas in your country, served by different ISPs, it could provide some protection against an ISP adversary. However, state-level adversaries could still have an advantage.
- Placing nodes in different countries (ideally in different ASes) will provide the greatest protection. However, note that it is still possible for collusion between entities such as ASes, which can reduce protection.

It's important to note that regardless of where you put these servers you can observe them, and if a client chooses your entrance and exit node, then the client is susceptible to attacks from you.
The Tor system has defense mechanism to reduce the chance of having both the

entrance and exit node under the control of the same entity.

From final exam 2019-2020



- The system works in rounds. In each round, mixes wait for a fixed period of time, then shuffle the messages they have received and forward them to the next layer or to the receivers.
- Assuming that there are N active users (N > 2) in the system, and Alice and Bob do not chat with anyone else in UMix, can an adversary who gains control over mixes 1 and 3 detect whether Alice and Bob talk to each other? Justify.

Controlling entry and exit mixes means that the adversary knows the senders and receivers of the messages. No other data is available as the messages are reordered, re-encrypted, and delayed by the middle mix.

The adversary can estimate when Alice and Bob talk to each other by their co-occurrence in the set of receivers and senders within a short time window. If the adversary has the capability to observe the communication over a long period of time, then they could mount a statistical disclosure attack. If Alice and Bob co-occur more often than they plausibly could due to dummies, then the adversary can be sure that they talk to each other. A specific mathematical model is worked out in the written exercises.

You want to set up a new online shop. You are really privacy-conscious, so you want to use privacy technologies to protect your customers from different angles.

To improve customer experience you want to add a chat where vendor and client can communicate. To protect customers' privacy, you want this channel to be anonymous. From the examples seen in the class, what kind of channel would you choose? Explain:

a) what privacy concern the channel protects from

b) under which threat model

c) why is it a better choice than the other channels