EPFL

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

CS-523 Advanced topics on Privacy Enhancing Technologies

Anonymous Communications Live exercises

Carmela Troncoso

SPRING Lab

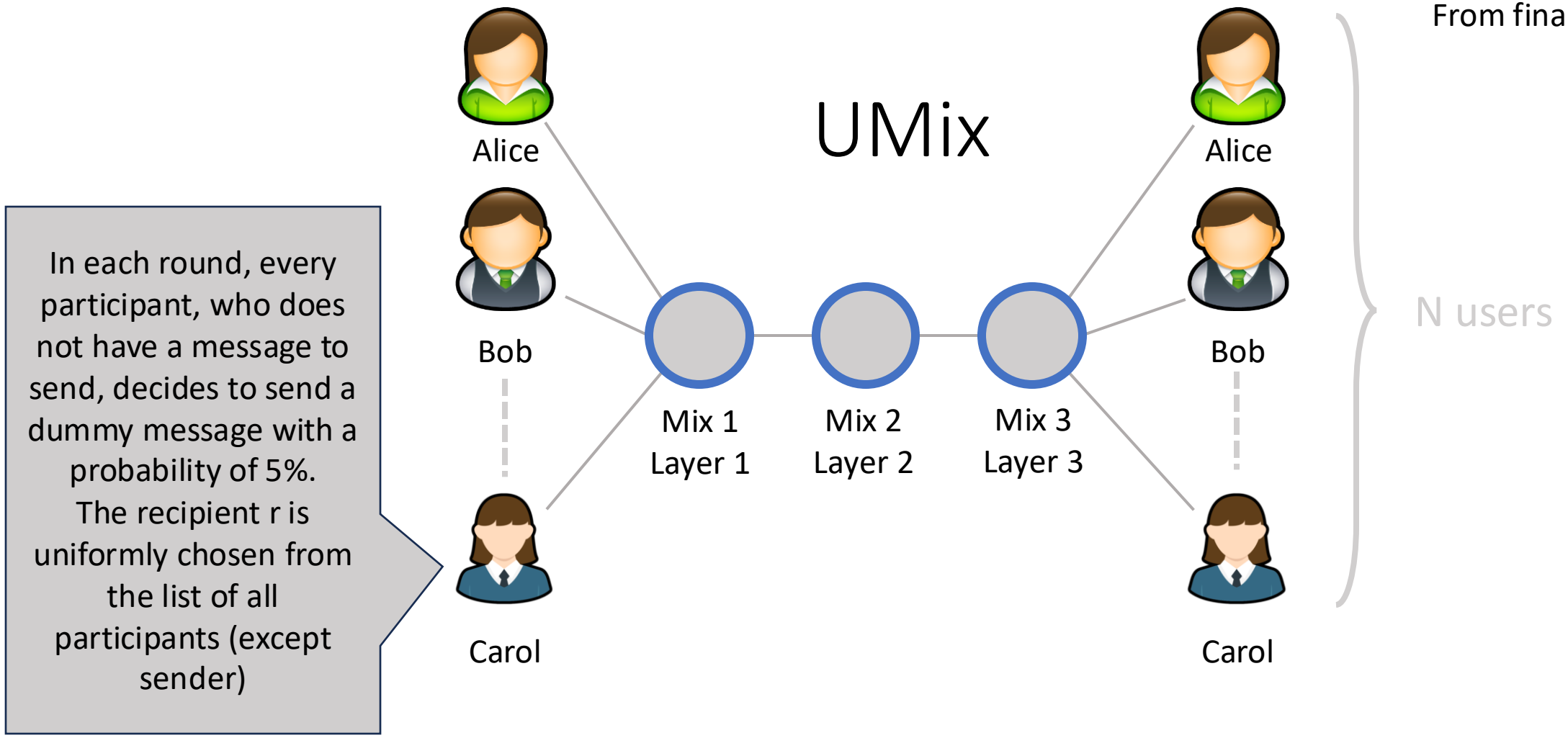
carmela.troncoso@epfl.ch

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.

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.

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