Group 17

Ben Korza

Mitchell Caisse

Mark Fitzgibbon

Conclusion

We have demonstrated that one can create a network that guarantees the anonymity of both its users and the content of the messages themselves. This network will allow users to communicate while simultaneously removing any association between them and their messages. We have shown that our system will route messages in a reasonable time and not saturate the network in stray packets. We have also illustrated that a system can be created in a peer-to-peer manner without the use of onion routing.

Our system only grants the user commands for sending messages and providing the name server with their port number. Future implementations could add more robust features like chat rooms, file sharing, and a way to distribute public and private keys. One could also create a protocol with conventions and functionality closer to that of an already familiar protocol like IRC.

* Future implementations can include multi-nameserver capabilities for improved scaling