

- a. **Team:**
- Sergey Frolov
 - Ian Martiny
 - Shirly Montero Quesada
- b. **Title:** OTR Messenger
- c. **Description:** A chat client that implements an Off-The-Record (OTR) protocol of communication. OTR allows clients to talk with each other in an encrypted fashion with repudiation – meaning a client can later deny having sent something.
- d. **Actors:**
- Clients – who can chat with each other;
 - Admin – who maintains the server
- e. **Functionality:**
- Clients can sign up
 - Clients can log in
 - Clients can send messages to other clients
 - Clients can receive messages sent from other clients
 - Clients can add other clients to their friends list by name
 - Clients can remove friends from their friends list
 - Clients can view their friends list
 - Admins can launch or terminate server
 - Clients can view their encryption and signing keys
 - Admins can query server for full list of clients
 - Admins print list of users
 - Admins can print the public key of a particular user
 - Admins can see statistics of server (debugging information)
 - Clients can instantiate the change of their encryption and signing keys
- f. **Stretch Functionality:**
- Working GUI
 - Clients can reset their login password
 - Clients can manually change their encryption and signing keys
 - Clients can add many users to their friends list by importing a contact list
 - Clients can attach files to their messages
 - Clients can blacklist other clients
 - Clients can read old messages
- g. **Considered Design Patterns:**
- Observer – for monitoring chat clients
 - Proxy – for setting up connections and relaying messages
 - Memento – for saving old conversations
 - Command (undo) – for deleting (and undoing the delete) conversations