OUR GOAL : [ To define and construct operations write,read, and attest to information that using secrets will not be discovered by any unintended principals ]

During Message Transfers:

* A message that is received must have not been tampered with or corrupted
* A message that is received must not have been replayed by an adversary
* A message that is sent/received must ensure that it is seen by the intended parties

At Login:

* On login, an adversary must not be able to log in as another principal
* A password must ensure a level of security such as to make dictionary attacks impossible

After Log In Not During Message Transfers

* A user must be able to invite only people on your friends list to a conference
* A user must only be able to see people who are your friends
* A user must see appropriately whether other users are online only when they are online
* A user must see appropriately whether other users are offline only when they are offline

Conferences between people that are separate from main conference:

* A message that is sent/received in these "sub-conferences" must be only seen by those who are entitled to a sub conference
* same as "DURING MESSAGE TRANSFERS"

Communication with server and database

Communication with server and client