Report

As a first step when developing this program we devided different parts of the system into classes since Dafny is an object-oriented language. The classes we came up with are Token, Door, User and EnrolmentStation. According to the description the EnrolmentStation should keep track of the users. Those are therefore placed in a set inside the EnrolementStation. The User itself holds a Token which is personal for that User. Therefore the Token contains information about the User's fingerprint. The Token also has a field that specifies if it is valid (bool by default true), since if the Token is used by the wrong User it will become invalid. The Token also has a clearance level to know which type of Doors it has access to. Therefore each Door has an attribute called required clearance level. The Token must have equal or greater clearance level than the Door in order to have access. Clearance levels are specified as constants (functions returning the same value) called HIGH, MEDIUM and LOW. No other clearance levels can be used than those according to our specification.

If a Token is used that has a lower clearance level than the one required for the Door it will not be opened and the Token will not be invalidated by this. The only way to make a Token invalid is if it is used by a User with the wrong fingerprint.

The Door also holds another attribute called alarmOn (bool). This is by default false, but if a Token is misused the description says that an alarm should sound. Therefore we have constraints ensuring that if the Token becomes invalid or is invalid when a User tries to enter a door (calls method EnterDoor) the alarmOn attribute will be set to true (and valid set to false). It will be in that way that when Token's attribute valid is true, alarmOn will be false and vice versa. Access to the Door is always denied if Token is invalid or if the clearance level isn’t high enough. Though access is granted only if Token is valid, the fingerprint matches the Token’s stored fingerprint and if the clearance level is sufficient.

ValidateClearanceLevel and ValidateFingerPrint are function methods since they are used in both the specification of method EnterDoor and in the implementation of it.

The EnrolmentStation has a method called Enrol. This method is used to register Users into the system. It takes as arguments a non-registered, non-null User that haven’t got any Token, a clearance level and a fingerprint. The clearance level and the fingerprint is stored into a Token that the User recieves. Afterwards the User is in the system, has a valid Token with the given clearance level and fingerprint.