

Contents

| | | |
|----------|-----------------------------|-----------|
| 1 | General | 2 |
| 1.1 | General Operators | 4 |
| 2 | Login | 8 |
| 3 | Student | 12 |
| 4 | Host | 13 |
| 5 | Administrator | 15 |
| 6 | Group Chat | 17 |
| 7 | Profile | 18 |

1 General

section *general* **parents** *homestay*

We want to have a few basic types here. We need to know general information about all of the users in the system:

- Email address, this is the unique identifier in the system
- Password, this has restrictions:
 - At least 8 characters in length
 - 1 digit
 - 1 uppercase character
 - 1 lowercase character
- First name, should be non-empty
- Last name, should be non-empty

$[Email, Password, FirstName, LastName]$

$Month ::= January$

| *February*

| *March*

| *April*

| *May*

| *June*

| *July*

| *August*

| *September*

| *October*

| *November*

| *December*

$Day == \mathbb{N}$

$Year == \mathbb{N}$

We want to know whether or not the user is an admin or not. This is used so that they get access to certain features in the application.

$AdminFlag ::=$

Admin

| *NotAdmin*

$$\begin{aligned}
\textit{InappropriateFlag} ::= & \\
& \textit{Zero} \\
& | \textit{First} \\
& | \textit{Second} \\
& | \textit{Third} \\
& | \textit{Remove}
\end{aligned}$$

Using these basic types we construct more complex types in the system. The applicant is the user of the system. Password tokens are used to reset the password.

$$\begin{aligned}
\textit{Applicant} &== \textit{Email} \times \textit{Password} \times \textit{FirstName} \times \textit{LastName} \times \textit{AdminFlag} \\
\textit{PToken} &== \mathbb{N} \times \textit{Email} \\
\textit{Date} &== \textit{Month} \times \textit{Day} \times \textit{Year} \\
\textit{IFlag} &== \textit{Email} \times \textit{InappropriateFlag}
\end{aligned}$$

We need to be able to notify the user of what is happening in the application. So, we enumerate the possible responses from actions taken.

$$\begin{aligned}
\textit{Response} ::= & \\
& \textit{InvalidToken} \\
& | \textit{PasswordResetSuccessful} \\
& | \textit{LoginSuccessful} \\
& | \textit{InvalidAvailability} \\
& | \textit{ValidAvailability}
\end{aligned}$$

We need to know about the host stuff.

$$\begin{aligned}
\textit{Smoking} &::= \textit{EnjoysSmoking} \mid \textit{NonSmoking} \\
\textit{Pets} &::= \textit{NoPets} \mid \textit{YesPets}
\end{aligned}$$

$$\begin{aligned}
\textit{Price} &== \mathbb{N} \\
\textit{Availability} &== \textit{Date} \times \textit{Date} \\
\textit{HostPreference} &== \textit{Applicant} \times \textit{Smoking} \times \textit{Pets} \\
\textit{Posting} &== \textit{HostPreference} \times \textit{Availability} \times \textit{Price}
\end{aligned}$$

Our initial state is just a bunch of empty sets.

| |
|---|
| <i>HomestayInitial</i> |
| <i>Applicants</i> : \mathbb{P} <i>Applicant</i> |
| <i>Emails</i> : \mathbb{P} <i>Email</i> |
| <i>Passwords</i> : \mathbb{P} <i>Password</i> |
| <i>Valid, Invalid</i> : \mathbb{P} <i>PToken</i> |
| <i>IFlags</i> : \mathbb{P} <i>IFlag</i> |
| <i>Postings</i> : \mathbb{P} <i>Posting</i> |
| <i>HostPreferences</i> : \mathbb{P} <i>HostPreference</i> |
| <i>Applicants</i> = \emptyset |
| <i>Emails</i> = \emptyset |
| <i>Passwords</i> = \emptyset |
| <i>Valid</i> = <i>Invalid</i> = \emptyset |
| <i>IFlags</i> = \emptyset <i>Postings</i> = \emptyset |
| <i>HostPreferences</i> = \emptyset |

In the database we need to ensure that there is each email address is unique, and that the password tokens are either valid or invalid.

| |
|---|
| <i>HomestayDatabase</i> |
| <i>HomestayInitial</i> |
| $\forall e_0, e_1 : \text{Email}; p_0, p_1 : \text{Password}; fn_0, fn_1 : \text{FirstName}; ln_0, ln_1 : \text{LastName} \bullet$ $e_0 = e_1 \Rightarrow (p_0 = p_1 \wedge fn_0 = fn_1 \wedge ln_0 = ln_1)$ $\text{Valid} \cap \text{Invalid} = \emptyset$ |

1.1 General Operators

It gets kind of silly to have to rewrite these operators and functions each time, so we have some helpers here.

We want an easy way to update an applicant. This helper function updates the applicant in the set of all applicants, identified by the email address.

| |
|---|
| $[X, Y, Z]$ |
| <i>firstOf3</i> == $\lambda x : X; y : Y; z : Z \bullet x$ |
| <i>secondOf3</i> == $\lambda x : X; y : Y; z : Z \bullet y$ |
| <i>thirdOf3</i> == $\lambda x : X; y : Y; z : Z \bullet z$ |

| |
|---|
| $[X, Y, Z]$ |
| <i>updateFirstOf3</i> : $(X \times Y \times Z) \times X \rightarrow X \times Y \times Z$ |
| $\forall xyz : X \times Y \times Z; x : X \bullet$ $\exists x_0 : X; y : Y; z : Z \mid xyz = (x_0, y, z) \bullet$ $\text{updateFirstOf3}(xyz, x) = (x, y, z)$ |

| $[X, Y, Z]$ |
|---|
| $updateSecondOf3 : (X \times Y \times Z) \times Y \rightarrow X \times Y \times Z$ |
| $\forall xyz : X \times Y \times Z; y : Y \bullet$ $\exists x : X; y_0 : Y; z : Z \mid xyz = (x, y_0, z) \bullet$ $updateSecondOf3(xyz, y) = (x, y, z)$ |

| $[X, Y, Z]$ |
|--|
| $updateThirdOf3 : (X \times Y \times Z) \times Z \rightarrow X \times Y \times Z$ |
| $\forall xyz : X \times Y \times Z; z : Z \bullet$ $\exists x : X; y : Y; z_0 : Z \mid xyz = (x, y, z_0) \bullet$ $updateThirdOf3(xyz, z) = (x, y, z)$ |

We're going to Greenspun up some stuff.

$Ord ::= LT \mid EQ \mid GT$

| $month2Nat : Month \rightarrow \mathbb{N}$ |
|--|
| $month2Nat \text{ January} = 1 \wedge$ $month2Nat \text{ February} = 2 \wedge$ $month2Nat \text{ March} = 3 \wedge$ $month2Nat \text{ April} = 4 \wedge$ $month2Nat \text{ May} = 5 \wedge$ $month2Nat \text{ June} = 6 \wedge$ $month2Nat \text{ July} = 7 \wedge$ $month2Nat \text{ August} = 8 \wedge$ $month2Nat \text{ September} = 9 \wedge$ $month2Nat \text{ October} = 10 \wedge$ $month2Nat \text{ November} = 11 \wedge$ $month2Nat \text{ December} = 12$ |

| $InFlag2Nat : InappropriateFlag \rightarrow \mathbb{N}$ |
|---|
| $InFlag2Nat \text{ Zero} = 0 \wedge$ $InFlag2Nat \text{ First} = 1 \wedge$ $InFlag2Nat \text{ Second} = 2 \wedge$ $InFlag2Nat \text{ Third} = 3 \wedge$ $InFlag2Nat \text{ Remove} = 4$ |

| |
|---|
| $Nat2InFlag : \mathbb{N} \rightarrow InappropriateFlag$ |
| $Nat2InFlag\ 0 = Zero \wedge$ |
| $Nat2InFlag\ 1 = First \wedge$ |
| $Nat2InFlag\ 2 = Second \wedge$ |
| $Nat2InFlag\ 3 = Third \wedge$ |
| $Nat2InFlag\ 4 = Remove$ |

function 42 leftassoc $(_ \otimes _)$

| |
|---|
| $_ \otimes _ : \mathbb{P} Applicant \times Applicant \rightarrow \mathbb{P} Applicant$ |
| $\forall a_1 : Applicant; as : \mathbb{P} Applicant \bullet$ $\exists p_0, p_1 : Password;$ $fn_0, fn_1 : FirstName;$ $ln_0, ln_1 : LastName;$ $ad_0, ad_1 : AdminFlag;$ $e : Email;$ $a_0 : Applicant \mid$ $a_1 = (e, p_1, fn_1, ln_1, ad_1) \wedge (a_0 = (e, p_0, fn_0, ln_0, ad_0) \in as) \bullet$ $as \otimes a_1 = (as \setminus \{a_0\}) \cup \{a_1\}$ |
| $updateHostPrefs : \mathbb{P} HostPreference \times HostPreference \rightarrow \mathbb{P} HostPreference$ |
| $\forall hp : HostPreference; hps : \mathbb{P} HostPreference \bullet$ $\exists hp_0 : HostPreference \mid$ $firstOf3\ hp_0 = firstOf3\ hp \bullet$ $updateHostPrefs(hps, hp) = (hps \setminus \{hp_0\}) \cup \{hp\}$ |

RemoveUser

$\Delta HomestayDatabase$

$A? : Applicant$

$E : Email$

$P : Password$

$FN : FirstName$

$LN : LastName$

$AF : AdminFlag$

$(E, P, FN, LN, AF) = A?$

$Applicants' = Applicants \setminus \{A?\}$

$Emails' = Emails \setminus \{E\}$

$HostPreferences' = HostPreferences$

$Passwords' = Passwords$

$Valid' = Valid$

$Invalid' = Invalid$

$Postings' = Postings$

2 Login

section *login* parents *general*

When we go to create a new account, we need some information from the user. We update all of our sets to reflect the new addition. After they have successfully created an account, they are taken to the main menu.

| |
|--|
| <i>CreateUserAccount</i> |
| $\Delta HomestayDatabase$ |
| $E? : Email$ |
| $FN? : FirstName$ |
| $LN? : LastName$ |
| $P? : Password$ |
| $E? \notin Emails$ |
| $Emails' = Emails \cup \{E?\}$ |
| $Passwords' = Passwords \cup \{P?\}$ |
| $Applicants' = Applicants \cup \{(E?, P?, FN?, LN?, NotAdmin)\}$ |
| $Valid' = Valid$ |
| $Invalid' = Invalid$ |
| $Postings' = Postings$ |
| $HostPreferences' = HostPreferences$ |

| |
|---|
| <i>CreateAdminAccount</i> |
| $\Delta HomestayDatabase$ |
| $E? : Email$ |
| $FN? : FirstName$ |
| $LN? : LastName$ |
| $P? : Password$ |
| $AD? : AdminFlag$ |
| $E? \notin Emails$ |
| $AD? = Admin$ |
| $Emails' = Emails \cup \{E?\}$ |
| $Passwords' = Passwords \cup \{P?\}$ |
| $Applicants' = Applicants \cup \{(E?, P?, FN?, LN?, AD?)\}$ |
| $Valid' = Valid$ |
| $Invalid' = Invalid$ |
| $Postings' = Posting$ |
| $HostPreferences' = HostPreferences$ |

A person can create either a user account, or they can create an admin account. The idea is that the admin account isn't something that you can

specify, but you must be given a link to sign up for. The link you follow gives the admin flag.

$$\text{CreateAccount} == \text{CreateUserAccount} \vee \text{CreateAdminAccount}$$

To login, a user needs to enter their email and password. At this point they are taken to the main menu.

| | |
|--|--|
| <i>Login</i> | |
| $\exists \text{HomestayDatabase}$ | |
| $E? : \text{Email}$ | |
| $P? : \text{Password}$ | |
| $FN : \text{FirstName}$ | |
| $LN : \text{LastName}$ | |
| $AD : \text{AdminFlag}$ | |
| $\text{Resp!} : \text{Response}$ | |
| $E? \in \text{Emails}$ | |
| $P? \in \text{Passwords}$ | |
| $(E?, P?, FN, LN, AD) \in \text{Applicants}$ | |
| $\text{Resp!} = \text{LoginSuccessful}$ | |

Users can reset their password if they forget it. We take an email address, generate a password token, then dish that off to the email address. The user then finds the email with the reset token/link and proceeds to reset their password.

This is supposed to be one more step of indirection so that the user wont have their password reset at random. Of course, if the email address is already compromised, it doesn't make much difference.

ForgotPassword

$\Delta HomestayDatabase$

$E? : Email$

$T! : PToken$

$ID : \mathbb{N}$

$P : Password$

$FN : FirstName$

$LN : LastName$

$AD : AdminFlag$

$E? \in Emails$

$(E?, P, FN, LN, AD) \in Applicants$

$ID = \# Valid + \# Invalid + 1$

$T! = ID \mapsto E?$

$Valid' = Valid \cup \{T!\}$

$Invalid' = Invalid$

$Applicants' = Applicants$

$Emails' = Emails$

$Passwords' = Passwords$

$Postings' = Postings$

$HostPreferences' = HostPreferences$

Once the user has the password token, they can enter their new password.
We let them know that the reset was successful.

ResetPassword

$\Delta \text{HomestayDatabase}$

$P?, P : \text{Password}$

$T? : \text{PToken}$

$\text{Resp!} : \text{Response}$

$ID : \mathbb{N}$

$E : \text{Email}$

$FN : \text{FirstName}$

$LN : \text{LastName}$

$AD : \text{AdminFlag}$

$\text{App}_0, \text{App}_1 : \text{Applicant}$

$T? \in \text{Valid}$

$E = \text{second } T?$

$\text{Valid}' = \text{Valid} \setminus \{T?\}$

$\text{Invalid}' = \text{Invalid} \cup \{T?\}$

$\text{App}_0 = (E, P, FN, LN, AD) \in \text{Applicants}$

$\text{App}_1 = (E, P?, FN, LN, AD)$

$\text{Applicants}' = \text{Applicants} \otimes \text{App}_1$

$\text{Resp!} = \text{PasswordResetSuccessful}$

$\text{Emails}' = \text{Emails}$

$\text{Passwords}' = \text{Passwords}$

$\text{Postings}' = \text{Postings}$

$\text{HostPreferences}' = \text{HostPreferences}$

3 Student

section *student* **parents** *general*

4 Host

section *host* parents *general*

The host section allows the user to view and modify preferences specific to hosting a location. There are some general preferences for each host, e.g. smoking, and pets. Then there are preferences for each host location, e.g. price and availability.

EditHostSmoking

$\Delta HomestayDatabase$

$H? : HostPreference$

$H : HostPreference$

$S? : Smoking$

$H? \in HostPreferences$

$H = updateSecondOf3(H?, S?)$

$HostPreferences' = updateHostPrefs(HostPreferences, H)$

$Applicants' = Applicants$

$Emails' = Emails$

$Passwords' = Passwords$

$Valid' = Valid$

$Invalid' = Invalid$

$Postings' = Postings$

EditHostPets

$\Delta HomestayDatabase$

$H?, H : HostPreference$

$P? : Pets$

$H? \in HostPreferences$

$H = updateThirdOf3(H?, P?)$

$HostPreferences' = updateHostPrefs(HostPreferences, H)$

$Applicants' = Applicants$

$Emails' = Emails$

$Passwords' = Passwords$

$Valid' = Valid$

$Invalid' = Invalid$

$Postings' = Postings$

$EditHostPreferences == EditHostSmoking \vee EditHostPets$

So long as the start date is before the end date, we consider the Availability to be valid.

| |
|--|
| $ValiDateGood$ $A? : Availability$ $Resp! : Response$ $Start, End : Date$ $Y_0, Y_1 : Year$ $M_0, M_1 : Month$ $D_0, D_1 : Day$ |
| $((M_0, D_0, Y_0), (M_1, D_1, Y_1)) = A?$ $(Y_0 < Y_1) \vee$ $(Y_0 = Y_1 \wedge month2Nat\ M_0 < month2Nat\ M_1) \vee$ $(Y_0 = Y_1 \wedge M_0 = M_1 \wedge D_0 < D_1)$ $Resp! = ValidAvailability$ |

If the start date is after the end date, then no bueno.

| |
|--|
| $ValiDateBad$ $A? : Availability$ $Resp! : Response$ $Start, End : Date$ $Y_0, Y_1 : Year$ $M_0, M_1 : Month$ $D_0, D_1 : Day$ |
| $((M_0, D_0, Y_0), (M_1, D_1, Y_1)) = A?$ $(Y_0 > Y_1) \vee$ $(Y_0 = Y_1 \wedge month2Nat\ M_0 > month2Nat\ M_1) \vee$ $(Y_0 = Y_1 \wedge M_0 = M_1 \wedge D_0 > D_1)$ $Resp! = InvalidAvailability$ |

$$ValiDate == ValiDateGood \vee ValiDateBad$$

5 Administrator

section *admin* **parents** *general*

Administrator login only needs to act like an inbox with "flag as inappropriate" or "accept/reject match" messages from students. The administrator will have a link to the group chat that is flagged and can add messages or end the chat if it is inappropriate. If the student and host decide to chat, once they send in their accept/reject match to the admin, the admin will have final approval to accept or reject the match.

$$\begin{aligned} MatchFlag ::= & \\ & Accept \\ & | Reject \end{aligned}$$
$$\begin{aligned} Message ::= & \\ & OneAccept \\ & | TwoAccepts \\ & | NoAccepts \\ & | Inappropriate \end{aligned}$$

| | |
|--|--|
| $AdminMatch : Message \rightarrow MatchFlag$ | |
| $AdminMatch \ OneAccept = Reject \wedge$ | |
| $AdminMatch \ NoAccepts = Reject \wedge$ | |
| $AdminMatch \ TwoAccepts = Accept$ | |

AdminInappropriate

$\Delta HomestayDatabase$

$M? : Message$

$E? : Email$

$I : IFlag$

$In, In2 : InappropriateFlag$

$M? = Inappropriate$

$\{E? \mapsto In\} = \{E?\} \triangleleft IFlags$

$In \neq Remove$

$In2 = Nat2InFlag((InFlag2Nat\ In) + 1)$

$IFlags' = IFlags \oplus \{E? \mapsto In2\}$

$In2 \neq Remove$

$Applicants' = Applicants$

$Emails' = Emails$

$Passwords' = Passwords$

$Valid' = Valid$

$Invalid' = Invalid$

InappropriateUser

$\Delta HomestayDatabase$

$M? : Message$

$E? : Email$

$I : IFlag$

$In, In2 : InappropriateFlag$

$RemoveUser$

$M? = Inappropriate$

$\{E? \mapsto In\} = \{E?\} \triangleleft IFlags$

$In \neq Remove$

$In2 = Nat2InFlag((InFlag2Nat\ In) + 1)$

$IFlags' = IFlags \oplus \{E? \mapsto In2\}$

$In2 = Remove$

6 Group Chat

section *group_{chat}* **parents** *general*

7 Profile

section *profile* **parents** *general*