Phd course on

Formal modelling and analysis of interactive systems

Part 5
Usability and Security

Cognitive Errors, Usability vs. Security, Groupware

Antonio Cerone

United Nations University

International Institute for Software Technology

Macau SAR China

email: antonio@iist.unu.edu

web: www.iist.unu.edu

Contents

Cognitive Errors

Cognitive Errors

- Postcompletion Error
  closure due to goal accomplishment results in failing to complete outstanding tasks

Cognitive Errors

- Postcompletion Error
  closure due to goal accomplishment results in failing to complete outstanding tasks
- Expectation Failure
  existing mental models lead to faulty expectations

Cognitive Errors

- Postcompletion Error
  closure due to goal accomplishment results in failing to complete outstanding tasks
- Expectation Failure
  existing mental models lead to faulty expectations
- Habituation-induced Error
  decrease in response to a stimulus after repeated presentations leads to wrong response

Cognitive Errors

- Postcompletion Error
  closure due to goal accomplishment results in failing to complete outstanding tasks
- Expectation Failure
  existing mental models lead to faulty expectations
- Habituation-induced Error
  decrease in response to a stimulus after repeated presentations leads to wrong response

$\Longrightarrow$ may sometimes be prevented using design principles

Postcompletion Error

Cognitive cause: closure due to goal accomplishment results in failing to complete outstanding tasks

Postcompletion Error

Cognitive cause: closure due to goal accomplishment results in failing to complete outstanding tasks

It emerges because of a rule allowing the user to stop once the goal is achieved

Postcompletion Error

Cognitive cause: closure due to goal accomplishment results in failing to complete outstanding tasks

It emerges because of a rule allowing the user to stop once the goal is achieved

Design Principle: goal should always be accomplished through the last task in a sequence of tasks

Postcompletion Error

Cognitive cause: closure due to goal accomplishment results in failing to complete outstanding tasks

It emerges because of a rule allowing the user to stop once the goal is achieved

Design Principle: goal should always be accomplished through the last task in a sequence of tasks

Error is still present if a warning after goal achieved remind the user to do the completions tasks

Expectation Failure

Cognitive cause: existing mental models lead to faulty expectations

Expectation Failure

Cognitive cause: existing mental models lead to faulty expectations

It emerges because of the user's response to the failed expectation is in dissonance with the required interaction

Expectation Failure

Cognitive cause: existing mental models lead to faulty expectations

It emerges because of the user's response to the failed expectation is in dissonance with the required interaction

Design Principle: no assumption should be made on user's expectations

Expectation Failure

Cognitive cause: existing mental models lead to faulty expectations

It emerges because of the user's response to the failed expectation is in dissonance with the required interaction

Design Principle: no assumption should be made on user's expectations

Error may still arise if a message informs the user about the actual required interaction

Habituation-induced Error

Cognitive cause: decrease in response to a stimulus after repeated presentations leads to wrong response

Habituation-induced Error

Cognitive cause: decrease in response to a stimulus after repeated presentations leads to wrong response

It emerges because of the user responds in an automatic way to the stimulus explicitly aiming to arouse attention

Habituation-induced Error

Cognitive cause: decrease in response to a stimulus after repeated presentations leads to wrong response

It emerges because of the user responds in an automatic way to the stimulus explicitly aiming to arouse attention

No General Design Principle!

Habituation-induced Error

Cognitive cause: decrease in response to a stimulus after repeated presentations leads to wrong response

It emerges because of the user responds in an automatic way to the stimulus explicitly aiming to arouse attention

No General Design Principle! But

- Context Specific Priciples (e.g. warnings should be used only when needed)
- Principle of Commensurate Effort may reduce the severity of the error consequences but does not reduce error likelihood

Unavoidable Subsidiary Tasks I

Unavoidable Subsidiary Tasks II

Closure: Exercise

How do you define the closure when you have more than one goal?

Model actions and closure for an ATM that allows to choose between

- cash withdrawal, and
- statements printing

Relations between Usability and Security

Usability: Def. and Aims

The ease of use and learnability of a human-made object.

[Wikipedia] (accessed in 2010)

Usability: Def. and Aims

> The ease of use and learnability of a human-made object.
>
> [Wikipedia] (accessed in 2010)

Should also aim to prevent user errors

Usability: Def. and Aims

> The ease of use and learnability of a human-made object.
>
> [Wikipedia] (accessed in 2010)

Should also aim to prevent user errors

Or at least to decrease likelihood or severity of user errors

Usability: Def. and Aims

> The ease of use and learnability of a human-made object.
>
> [Wikipedia] (accessed in 2010)

Should also aim to prevent user errors

Or at least to decrease likelihood or severity of user errors, which may lead to

- system failure
- catastrophic consequences

Usability vs. Security

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability
- Secure Usability

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability
- Secure Usability
  - poor usability decrease security

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability
- Secure Usability
  - poor usability decrease security
  - usability should increase security

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability
- Secure Usability
  - poor usability decrease security
  - usability should increase security
  - usability may decrease security

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability
- Secure Usability
  - poor usability decrease security
  - usability should increase security
  - usability may decrease security

$\Longrightarrow$ security mechanisms may decrease usability
$\Longrightarrow$ poor usability $\Longrightarrow$ decrease security

Usability vs. Security

- Usable Security
  - security mechanisms may decrease usability
- Secure Usability
  - poor usability decrease security
  - usability should increase security
  - usability may decrease security

$\Longrightarrow$ security mechanisms may decrease usability

$\Longrightarrow$ poor usability $\Longrightarrow$ decrease security

$\Longrightarrow$ security mechanisms may decrease security

Groupware Case Study

Groupware

Term for applications written to implement

- Computer-supported cooperative work (CSWC)

Groupware

Term for applications written to implement

- Computer-supported cooperative work (CSWC)

HCI $\Longrightarrow$ single user
multidisciplinary around axis
psychology–computing

Groupware

Term for applications written to implement

- Computer-supported cooperative work (CSWC)

HCI $\Longrightarrow$ single user
multidisciplinary around axis
psychology–computing

CSWC $\Longrightarrow$ group of users
multidisciplinary around axis
sociolology–computing

Groupware

Term for applications written to implement

- Computer-supported cooperative work (CSWC)

HCI $\Longrightarrow$ single user
multidisciplinary around axis
psychology–computing

CSWC $\Longrightarrow$ group of users
multidisciplinary around axis
sociolology–computing
$\Longrightarrow$ security issues

Case Study: Web Interface

A conference support web-basd tool that

- provides information on the event
- establishes a community via registration
- enables users to share their ideas, interests, etc. via discussion forum
- facilitates communication between users via creation of personal profiles

Web Design

Home

Forum

User Profiles

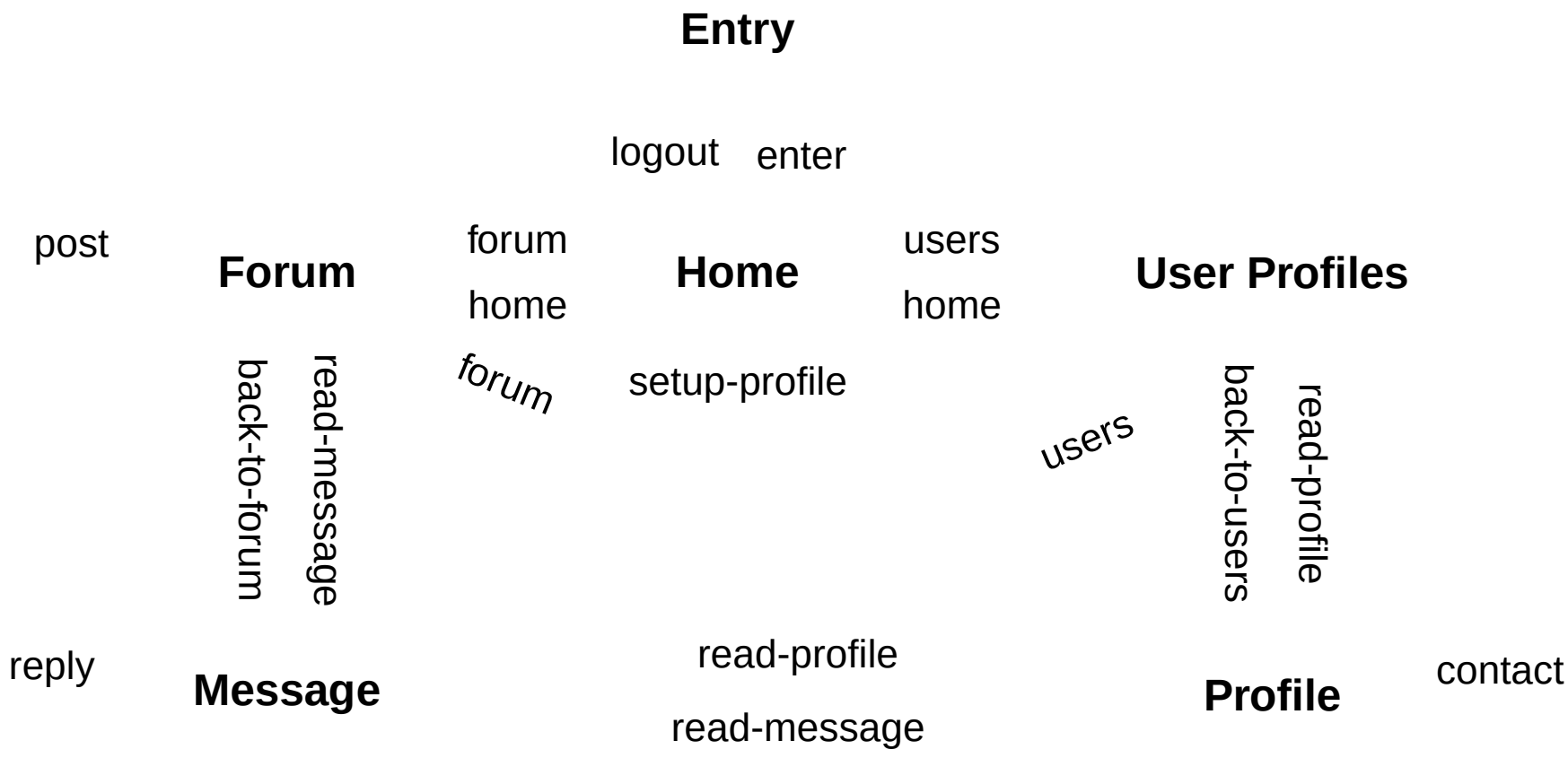
Message

Profile

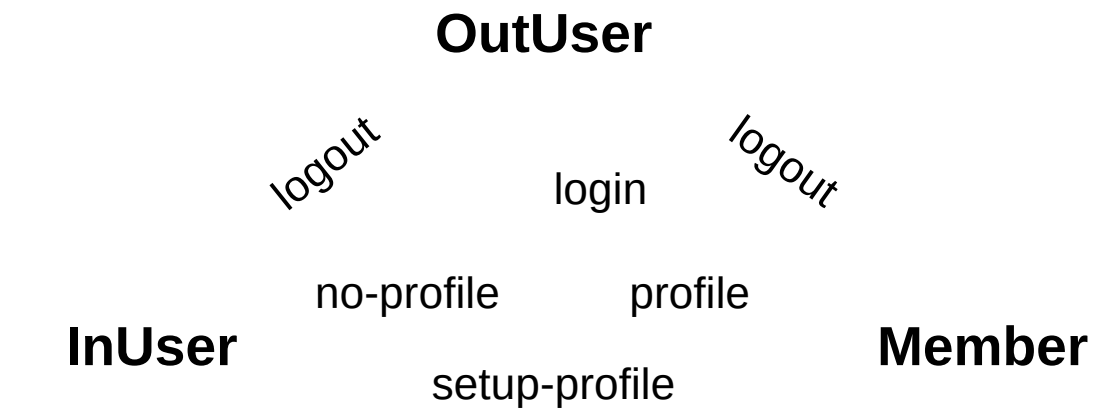
Web Pages

- Home to provide general information and materials about the conference and to set up own profile
  - Forum to browse posted messages and to post new messages
    - Message to analyse a posted message (possibly looking at the sender's profile), and post a reply to it
  - User Profiles to browse users' profiles
    - Profile to analyse other users'profiles (possibly looking at the messages they sent), and contact matching users

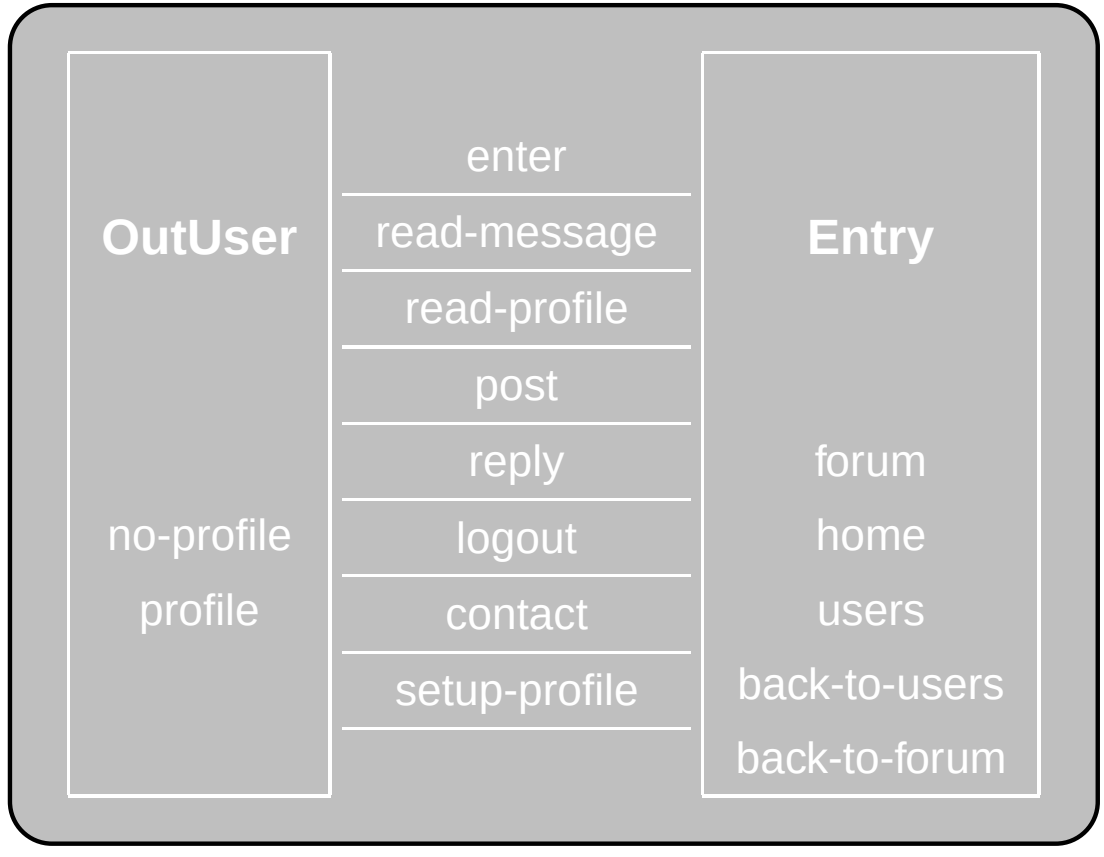
Web Interface



User Privileges



Interface



OutUser ‖ **Entry**

User Behaviour

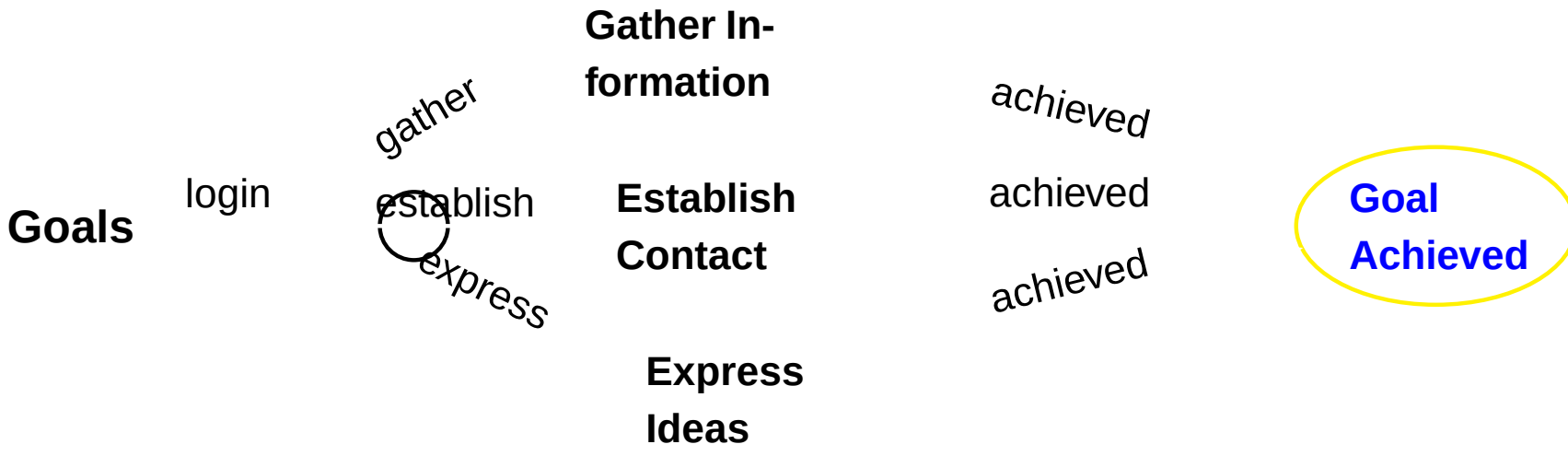
User: A conference participant

Scenario: The persona tries to

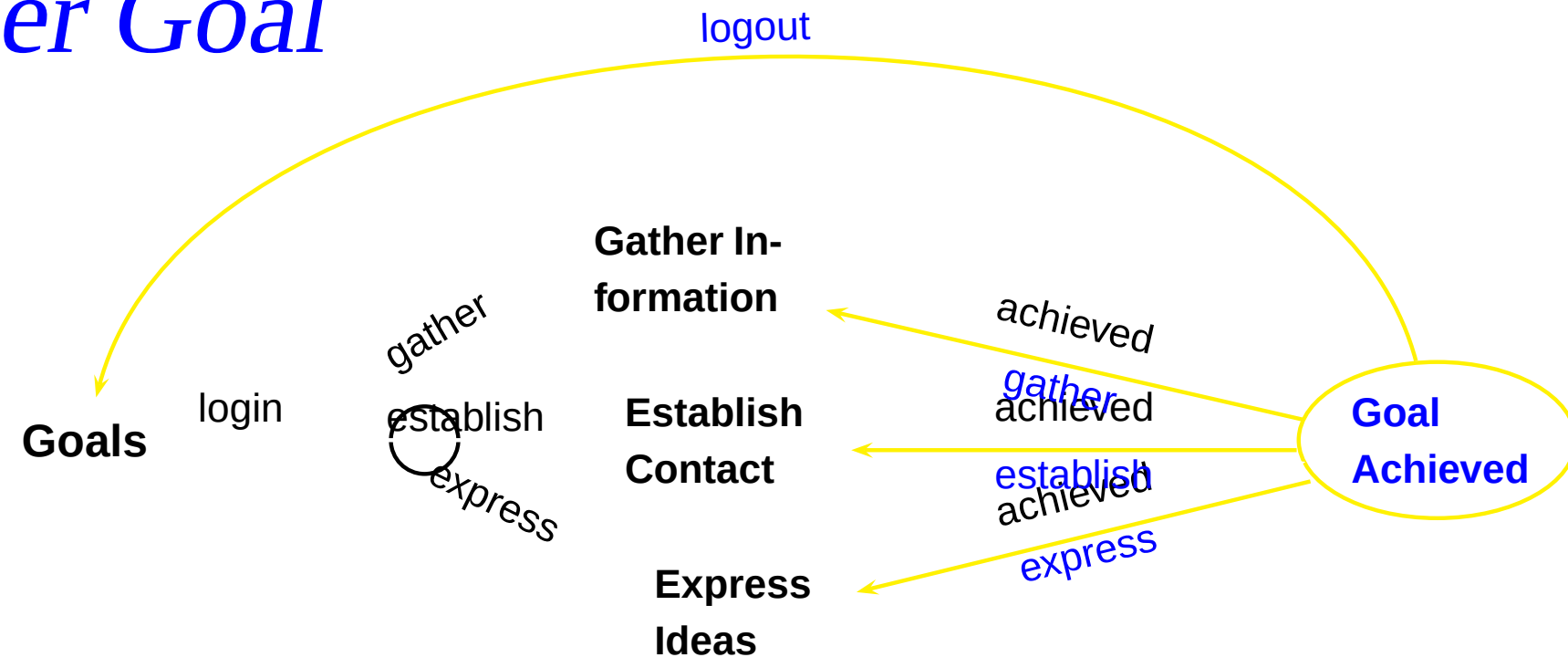
- gather information
- find/contact other users
- express his/her ideas

using the website.

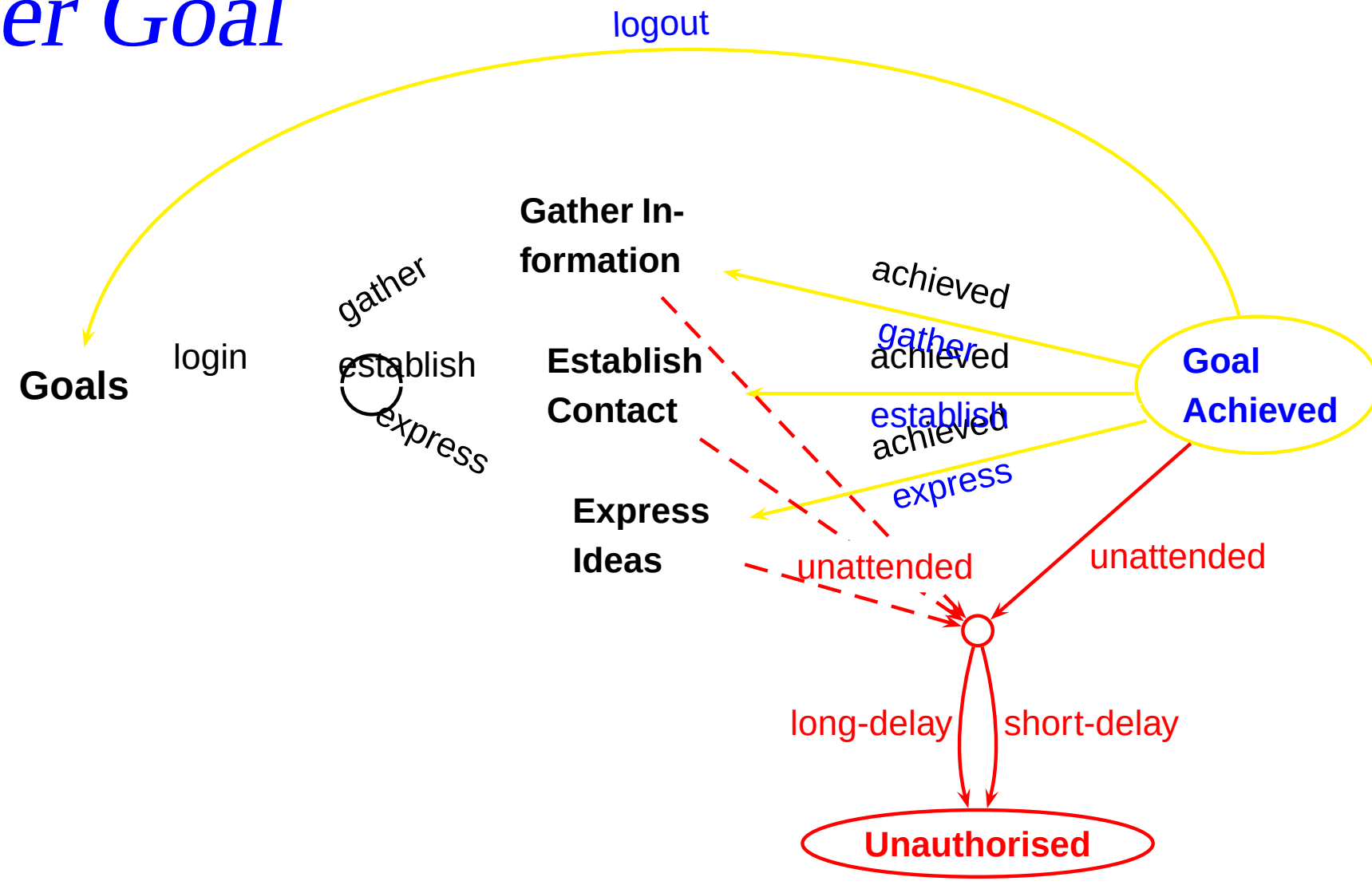
User Goal


Goals
login
gather
establish
express
Gather In-formation
Establish Contact
Express Ideas
achieved
achieved
achieved
Goal Achieved

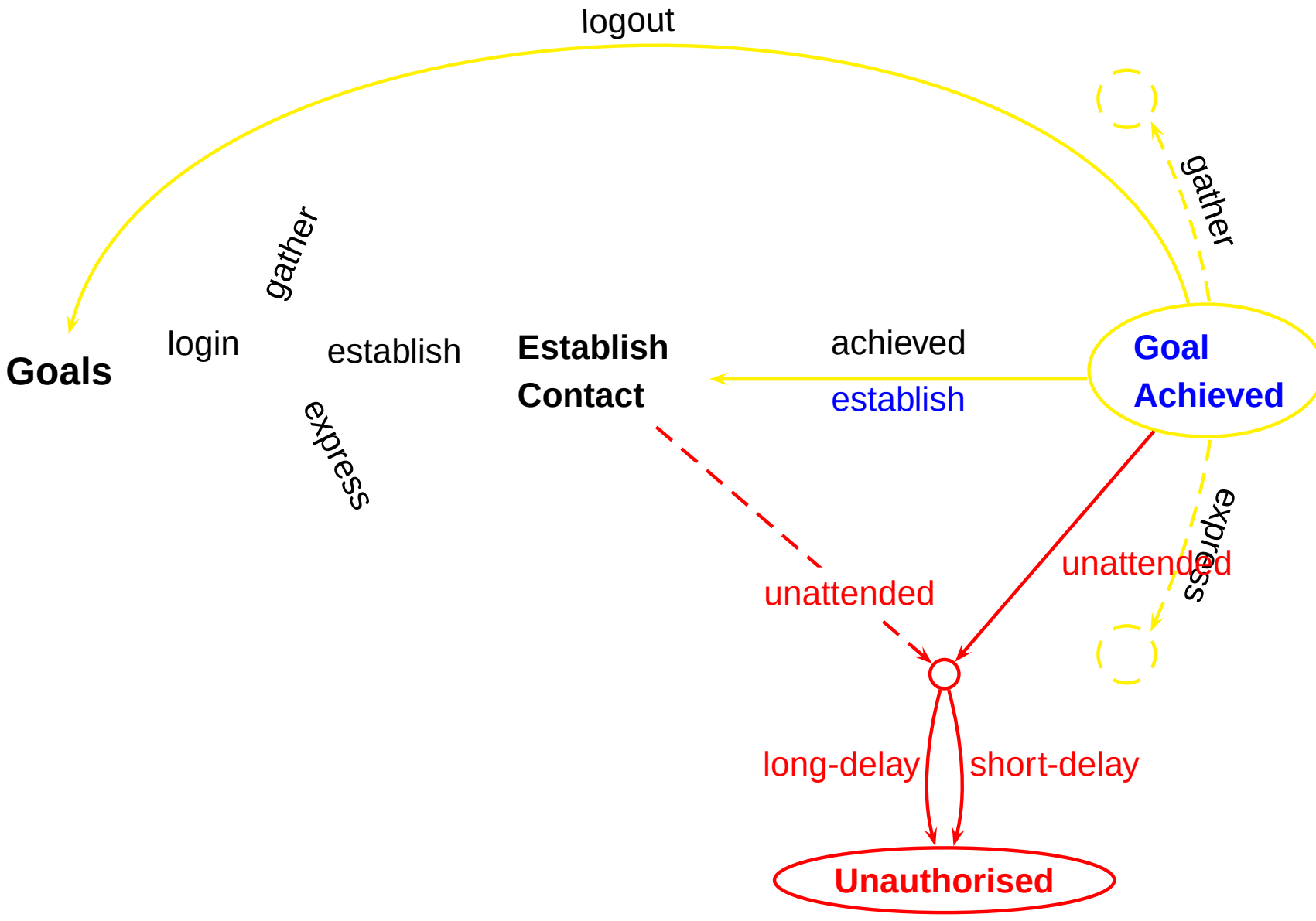
User Goal


logout
Goals
login
gather
establish
express
Gather In-
formation
Establish
Contact
Express
Ideas
achieved
gather
achieved
establish
achieved
express
Goal
Achieved

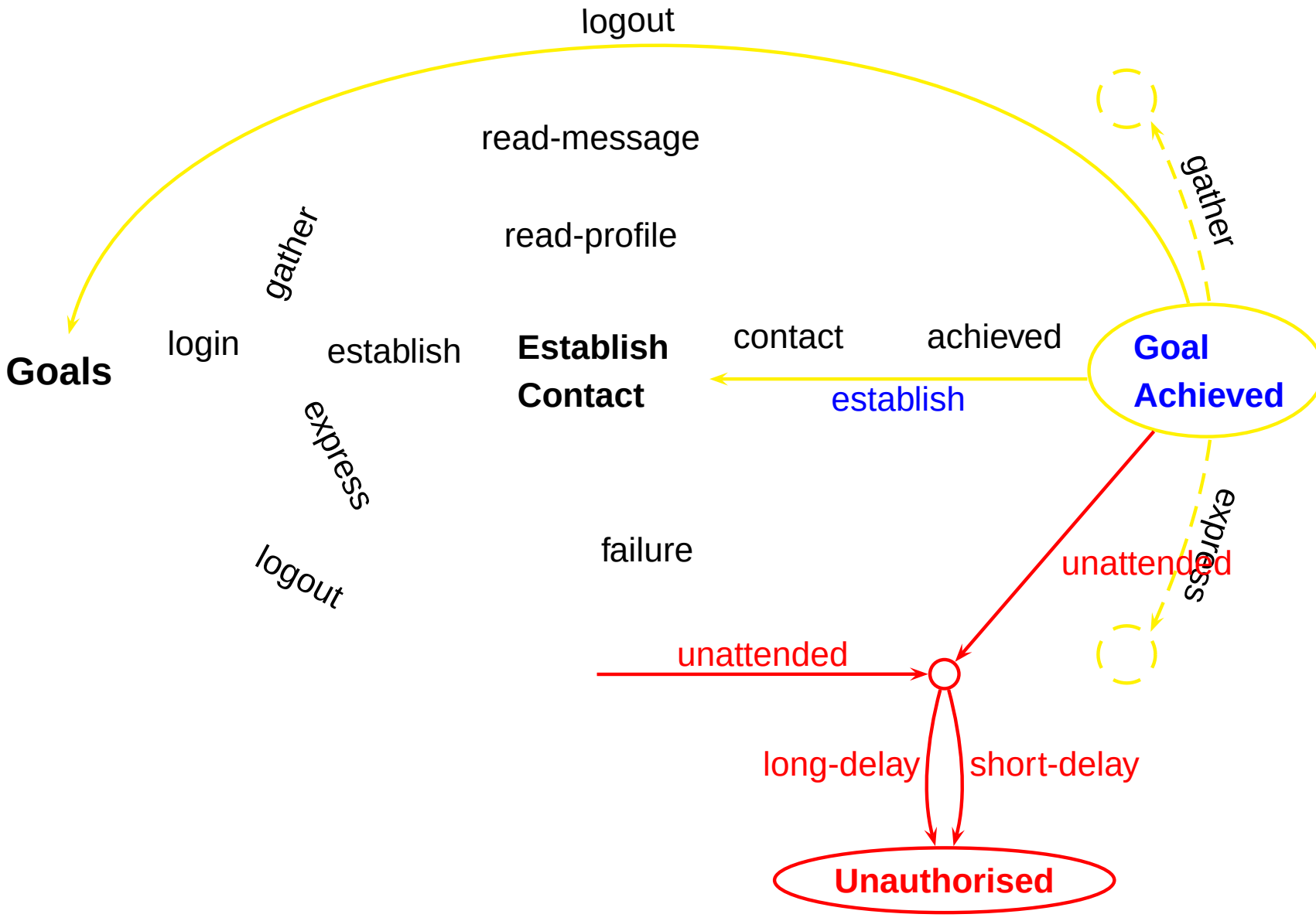
User Goal


logout
Goals
login
gather
establish
express
Gather In-
formation
Establish
Contact
Express
Ideas
achieved
gather
achieved
establish
achieved
express
Goal
Achieved
unattended
unattended
long-delay
short-delay
Unauthorised

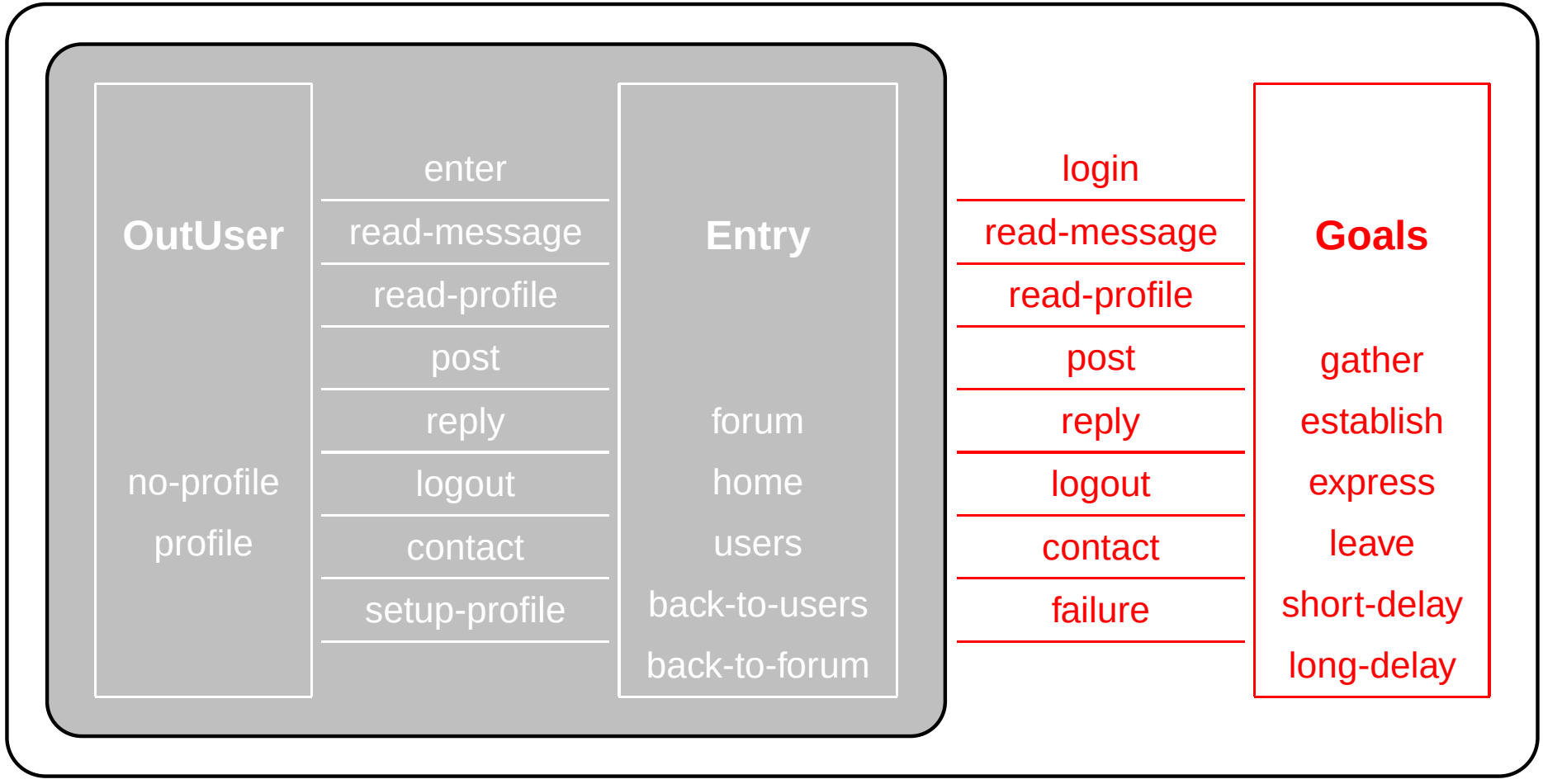
Establish Contact



Establish Contact



The Overall System



SYSTEM = (**OutUser** [| ... |] **Entry**) [| { login , ... , failure } |] **Goals**

Group of Users

Interaction Aspects

- local group of users
  interacting with a single shared interface
  rather than
  distributed group of users
  interacting among each other through the system

Group of Users

Interaction Aspects

- local group of users
  interacting with a single shared interface
  rather than
  distributed group of users
  interacting among each other through the system
- sequence of users

Group of Users

Interaction Aspects

- local group of users
  interacting with a single shared interface
  rather than
  distributed group of users
  interacting among each other through the system
- sequence of users

Security Aspects

- distinct users may have different privileges

Group of Users

Interaction Aspects

- local group of users
  interacting with a single shared interface
  rather than
  distributed group of users
  interacting among each other through the system
- sequence of users

Security Aspects

- distinct users may have different privileges
- users may act as authorised or unauthorised

Authorised vs. Unauthorised

Actions are attempted and may result in

- either success
- or failure

Authorised vs. Unauthorised

Actions are attempted and may result in

- either success
- or failure

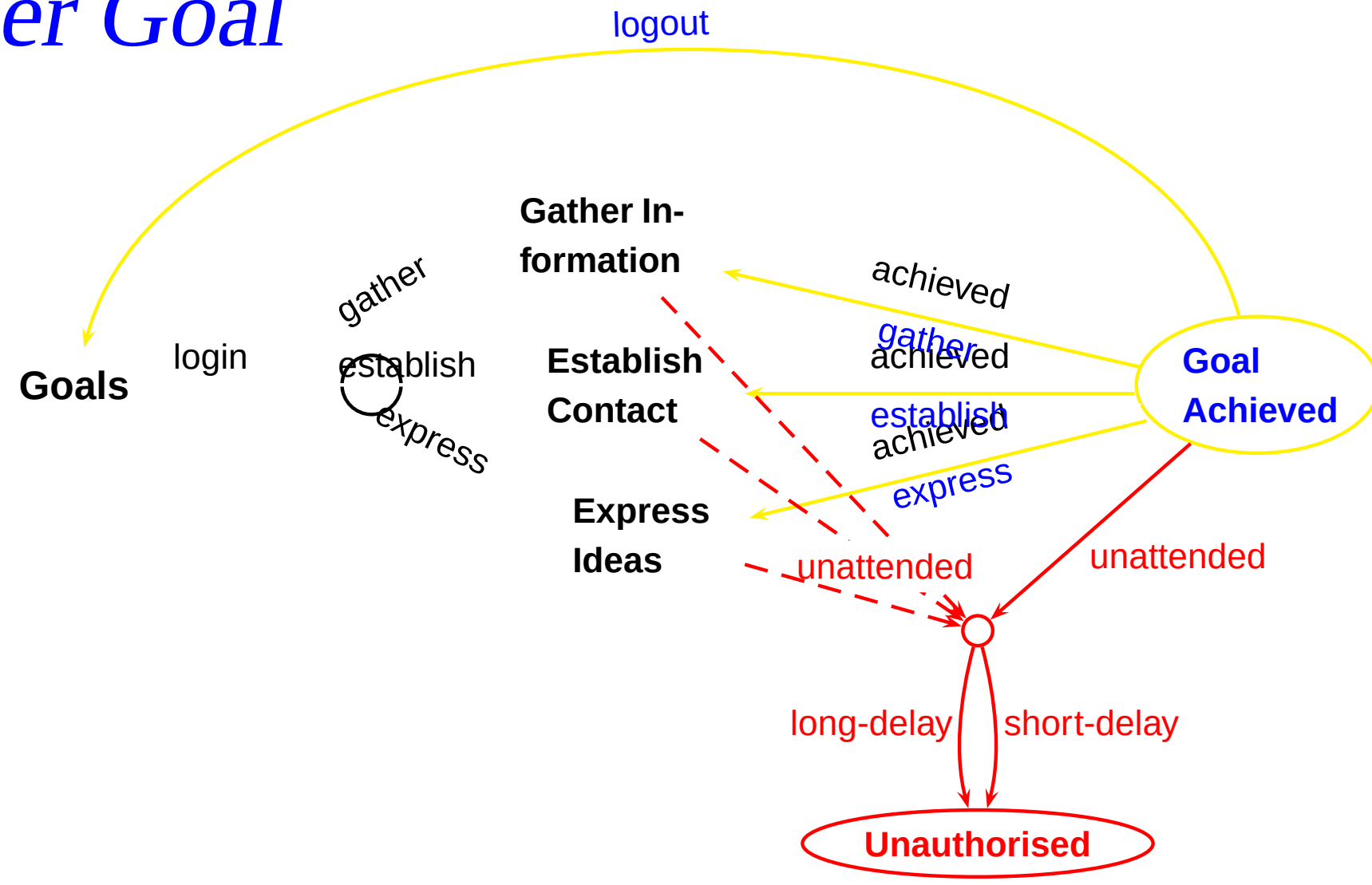
Authorised User

- is supposted to result in success

Unauthorised User

- is supposted to result in failure

User Goal


logout
Goals
login
gather
establish
express
Gather In-
formation
Establish
Contact
Express
Ideas
achieved
gather
achieved
establish
achieved
express
Goal
Achieved
unattended
unattended
long-delay
short-delay
Unauthorised

Strong Security

The property of strong security is expressed as follows

If the goal is achieved then user actions

- either never result in success (unauthorised user)
- or do not result in success until the user establish a new goal or performs a logout (authorised user)

Strong Security

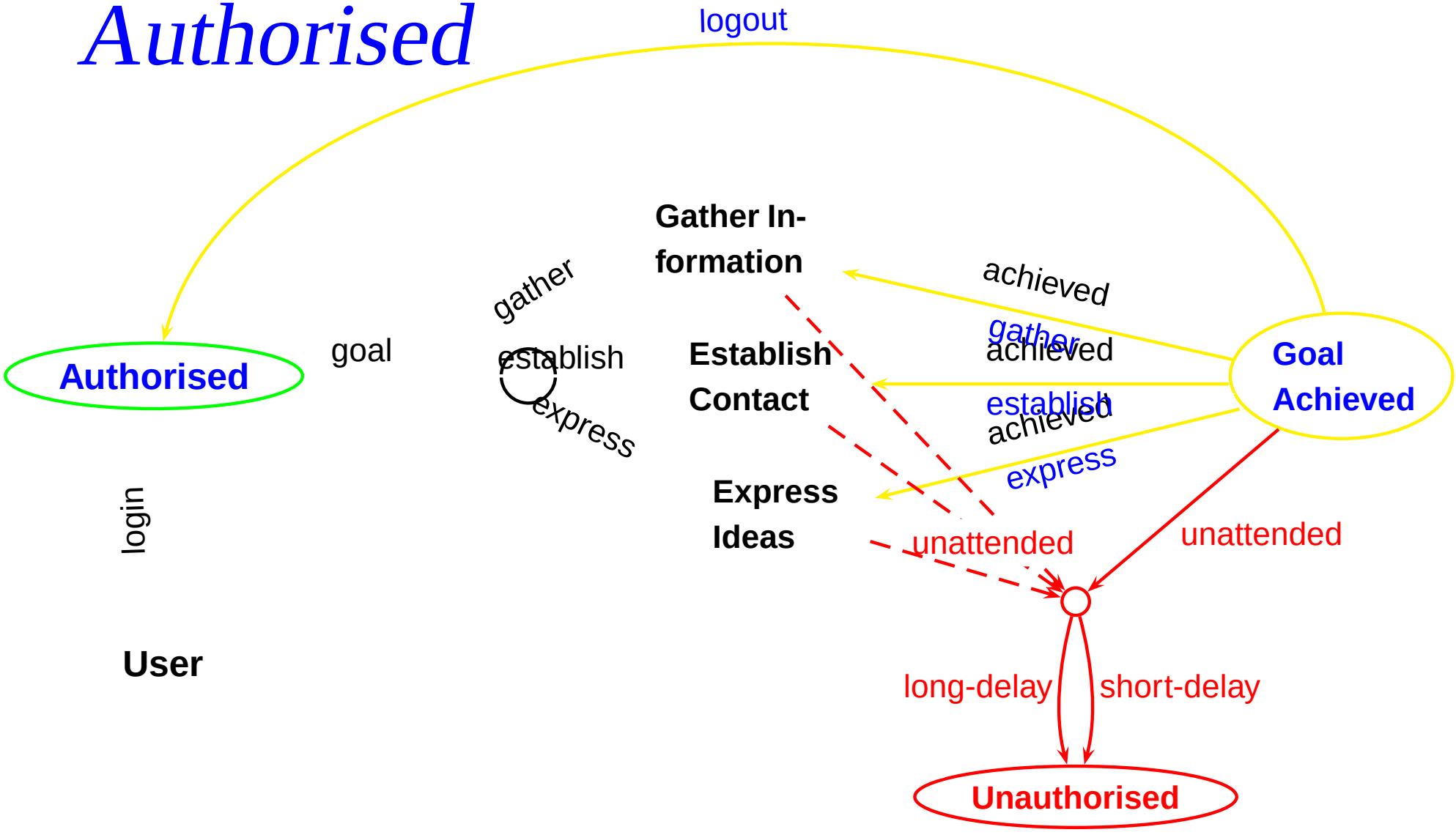
The property of strong security is expressed as follows

If the goal is achieved then user actions

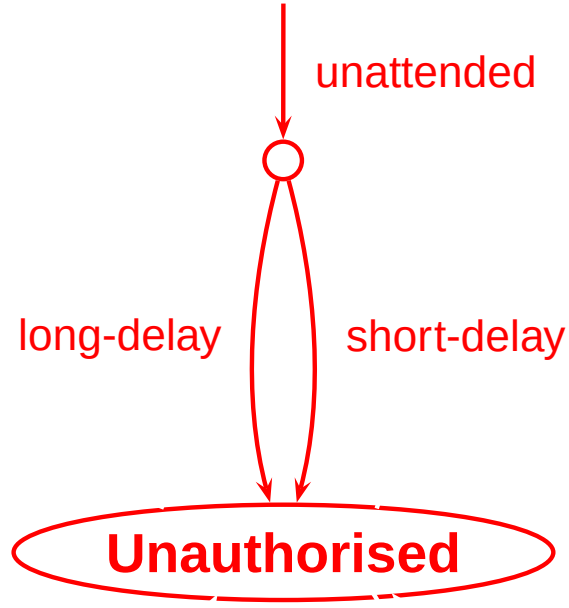
- either never result in success (unauthorised user)
- or do not result in success until the user establish a new goal or performs a logout (authorised user)

$$\Box achieved \rightarrow (\neg success \, \mathcal{W} \, (goal \vee logout))$$

Authorised


logout
Authorised
goal
gather
establish
express
Gather In-
formation
Establish
Contact
Express
Ideas
achieved
gather
achieved
establish
achieved
express
Goal
Achieved
unattended
unattended
long-delay
short-delay
Unauthorised
login
User

Unauthorised User



User

logout

read-message

read-profile

post

reply

contact

success

failure

Non Expert User

back-to-forum
back-to-users
home
users
forum
unattended
logout

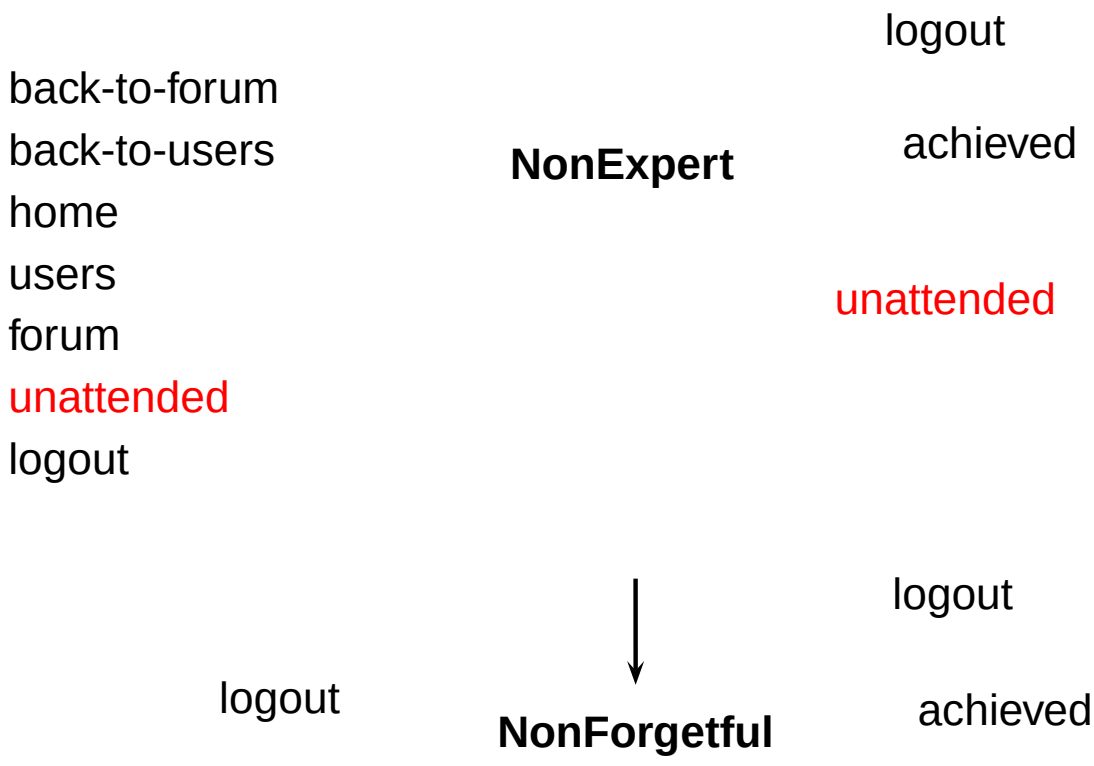
NonExpert

logout

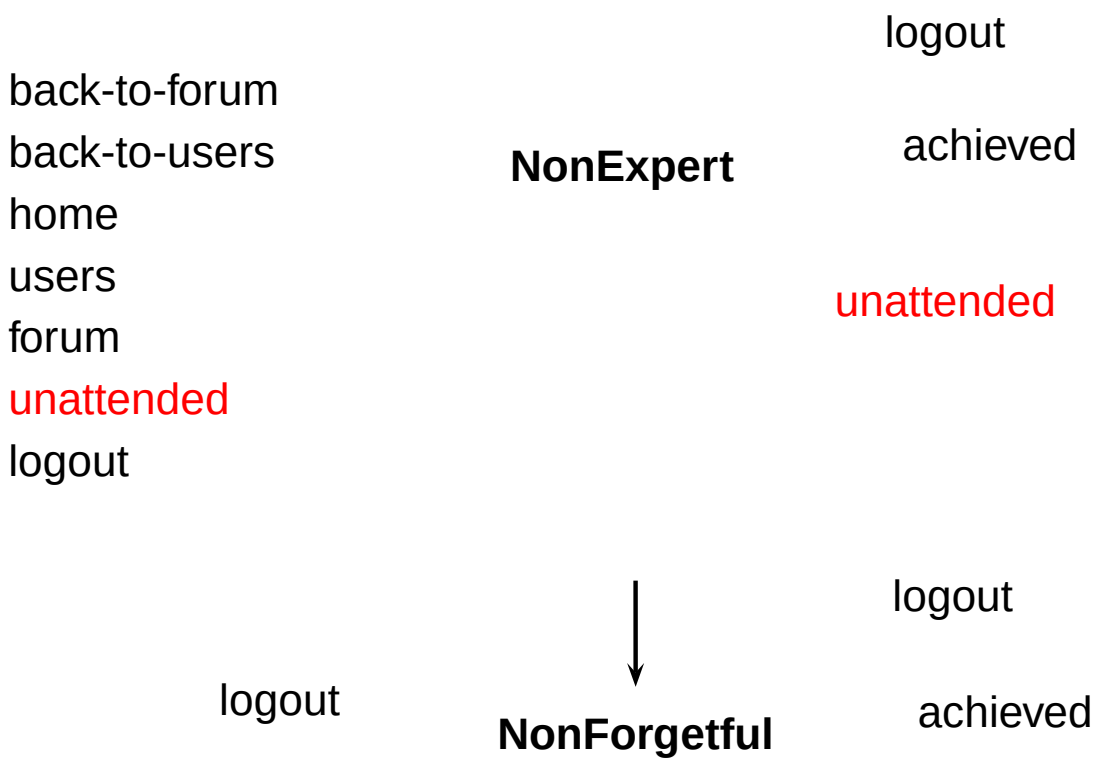
achieved

unattended

NonForgetful Users

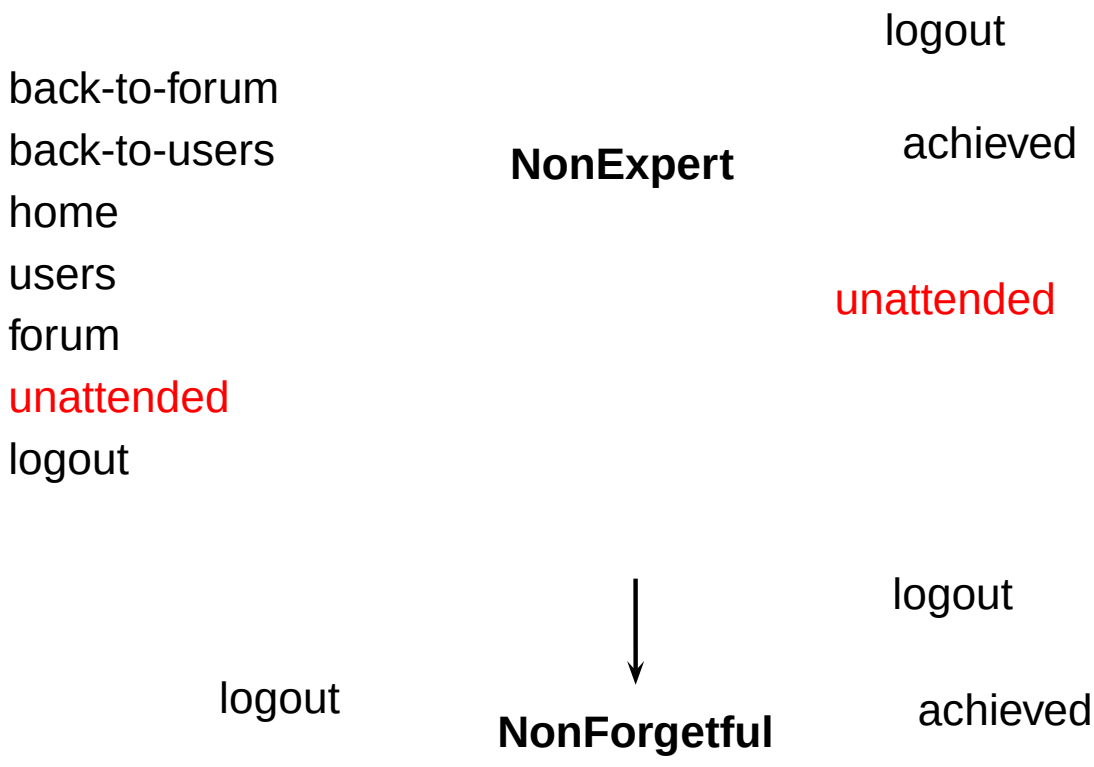


NonForgetful Users



(**SYSTEM** ‖ **NonExpert**) [| { achieved, logout, unattended } |] **NonForgetful**

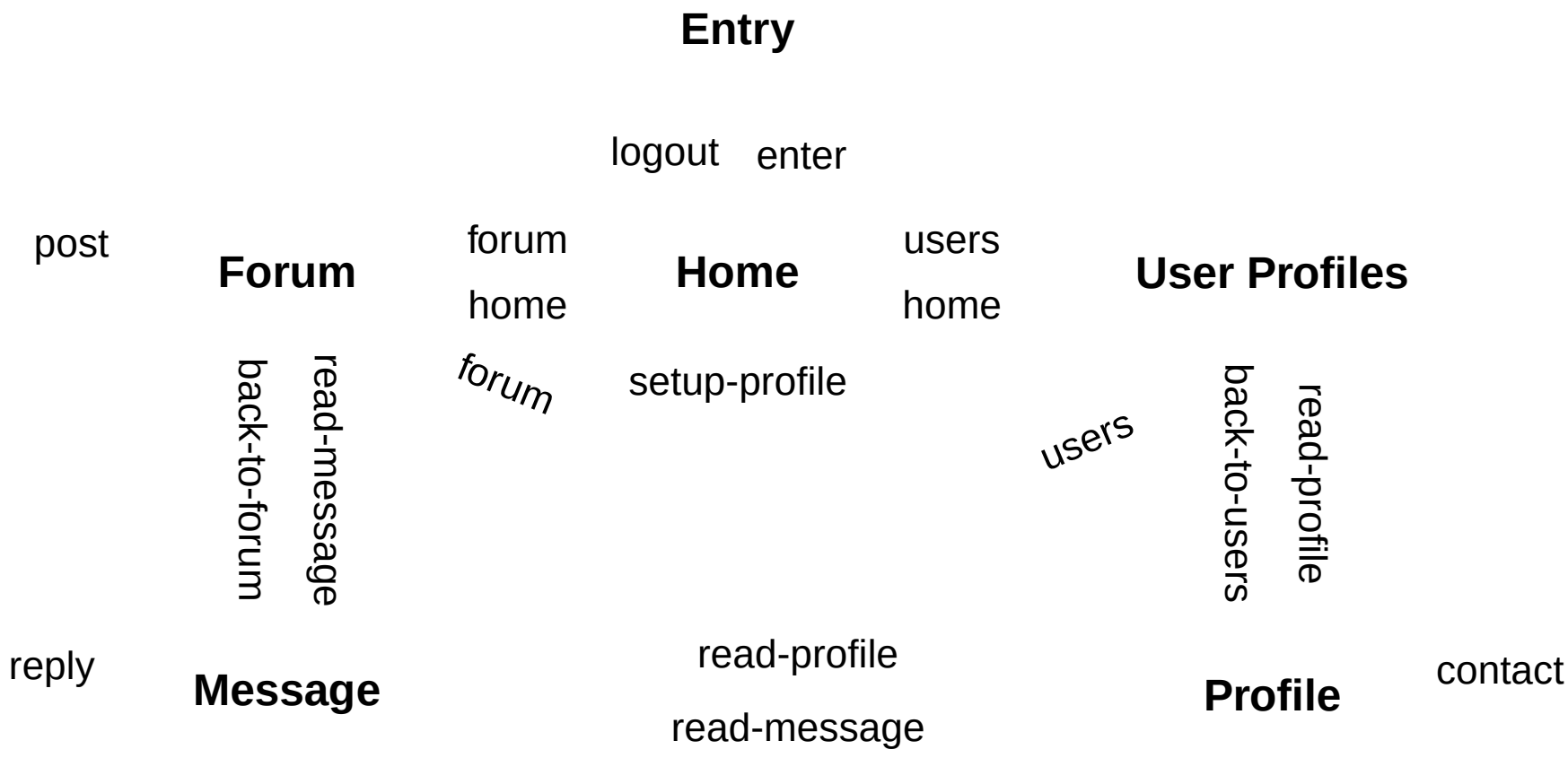
NonForgetful Users



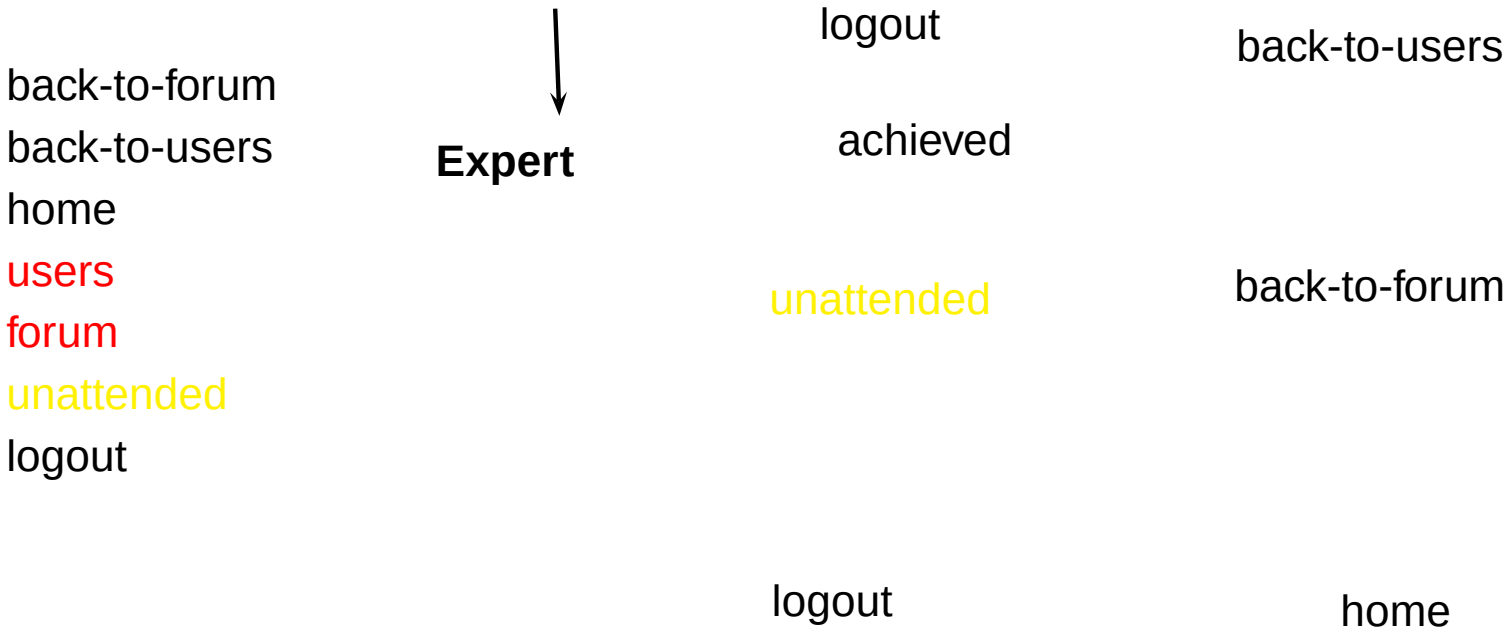
(**SYSTEM** ‖ **NonExpert**) [| { achieved, logout, unattended } |] **NonForgetful**

- The property does not hold!

Web Interface



Expertise



(SYSTEM || Expert)

Expertise

back-to-forum
back-to-users
home
users
forum
unattended
logout

NonExpert

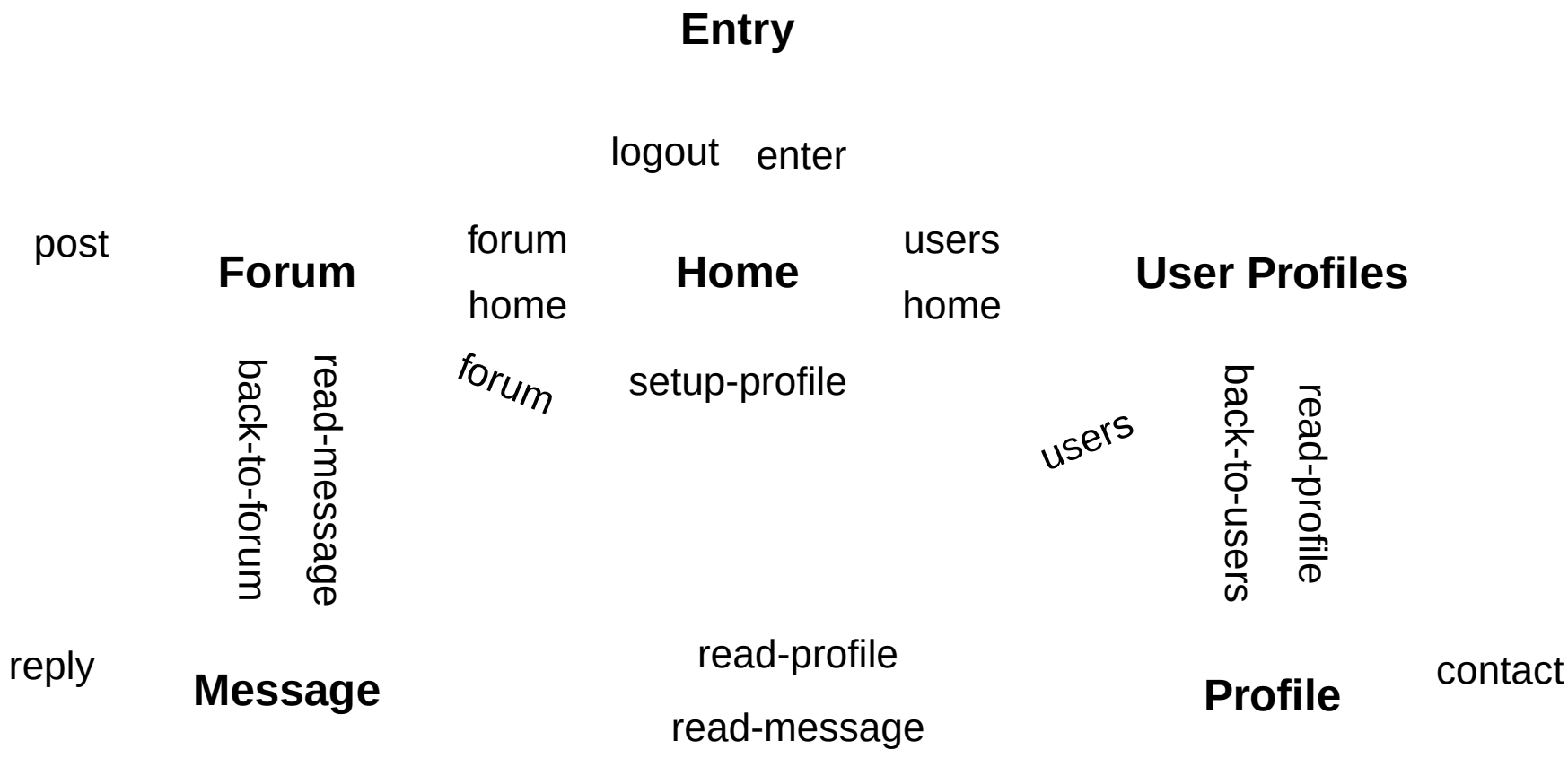
logout

achieved

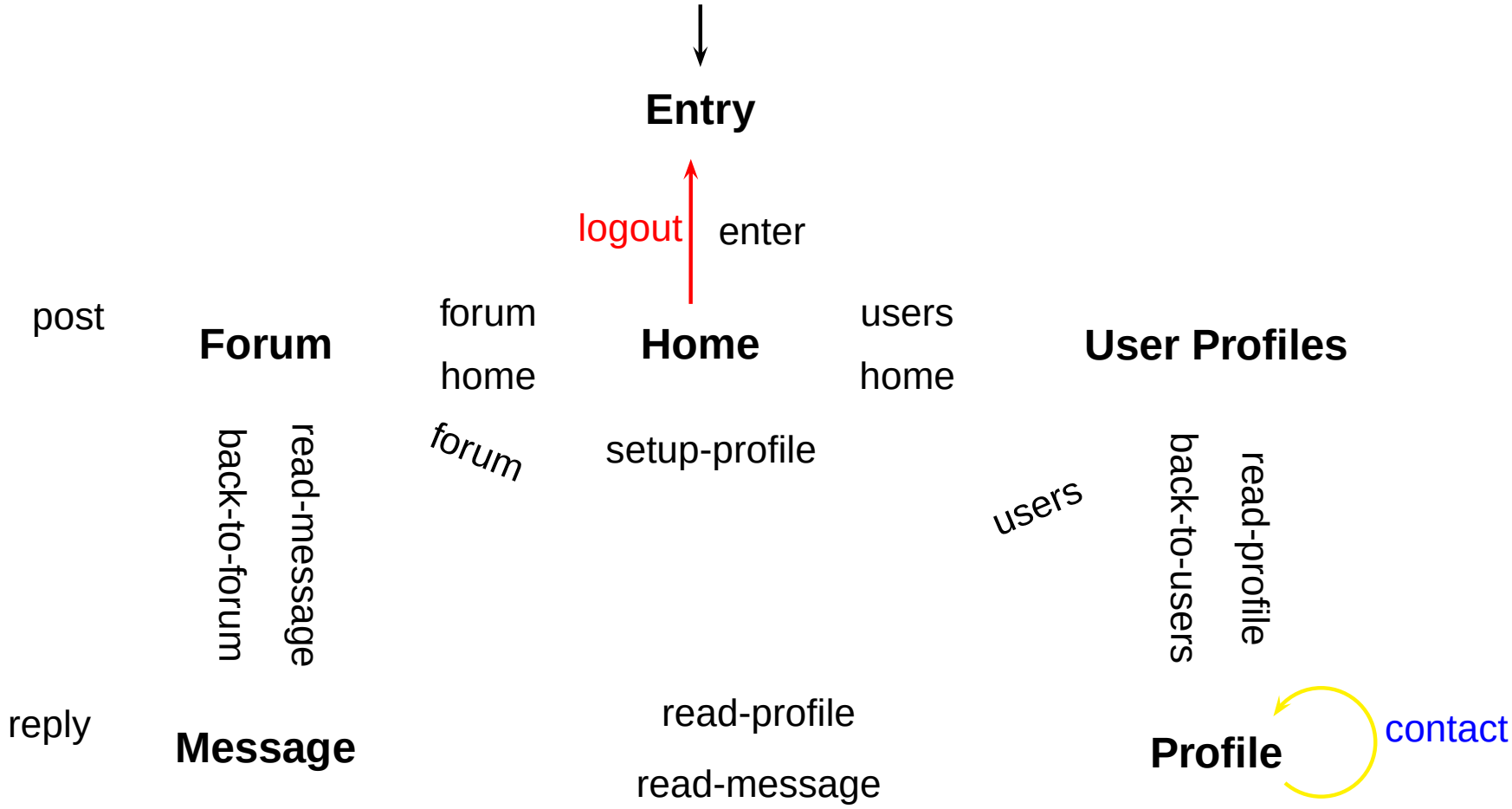
unattended

(SYSTEM || NonExpert)

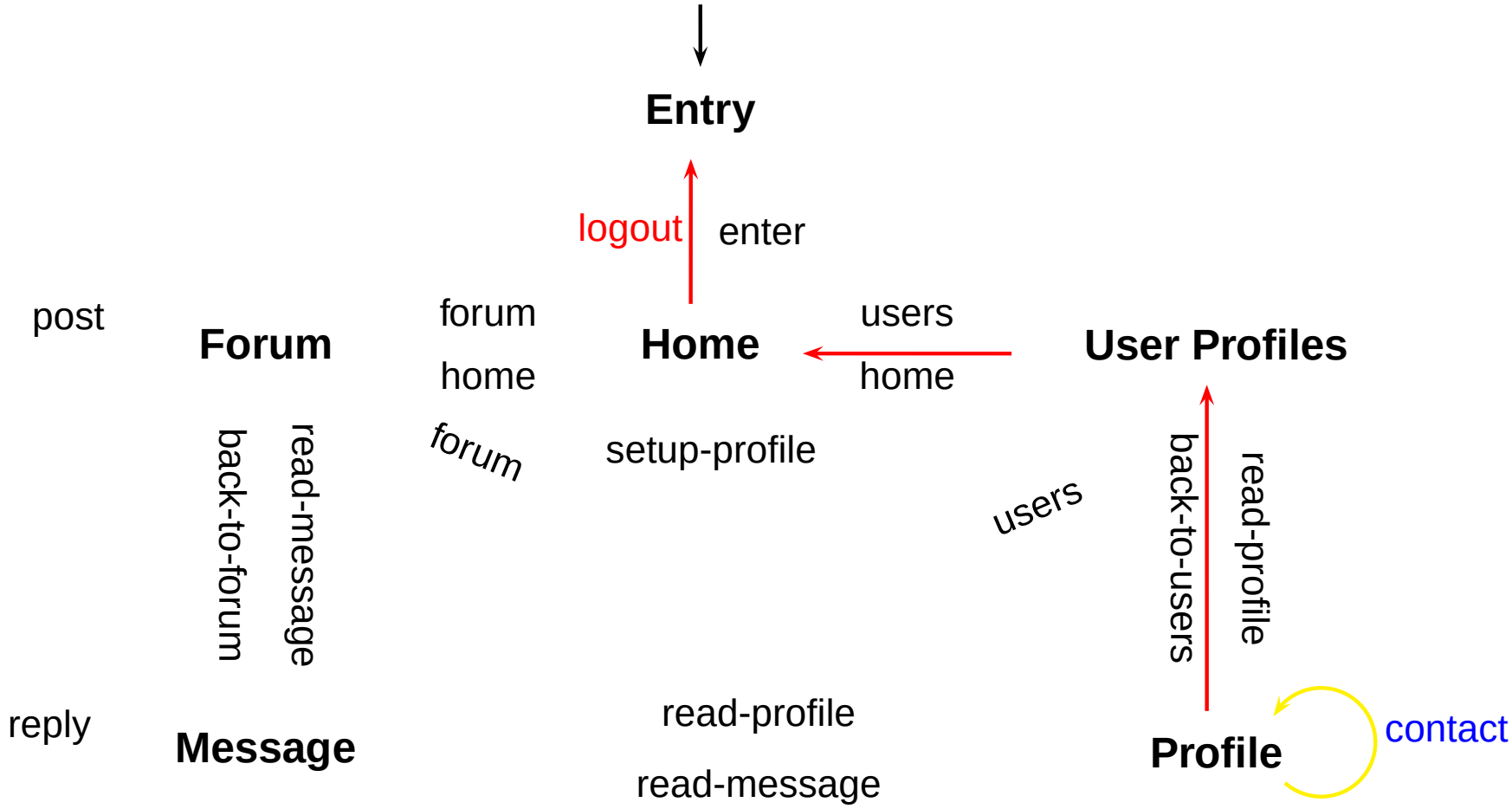
Web Interface



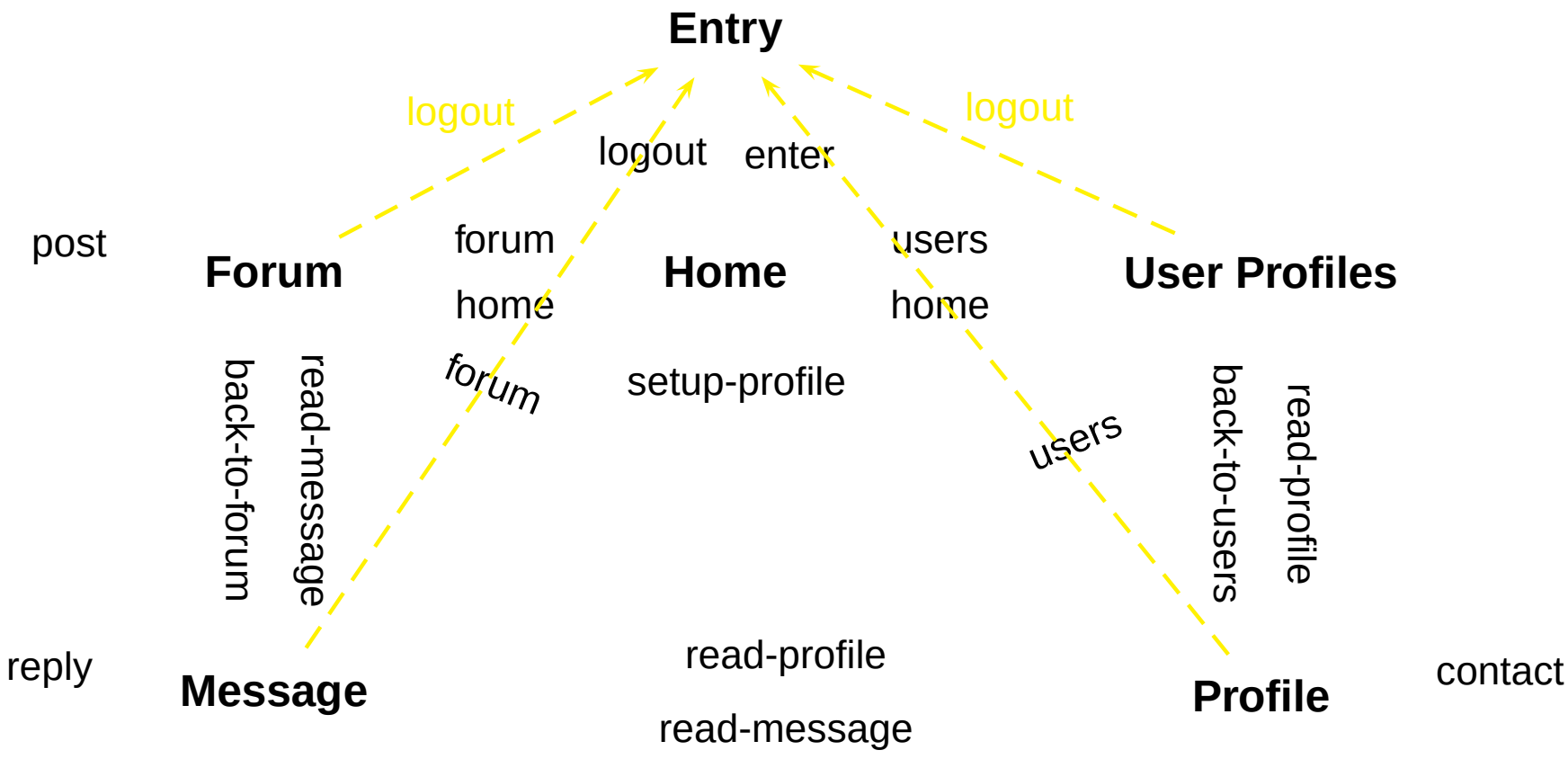
Web Interface 1



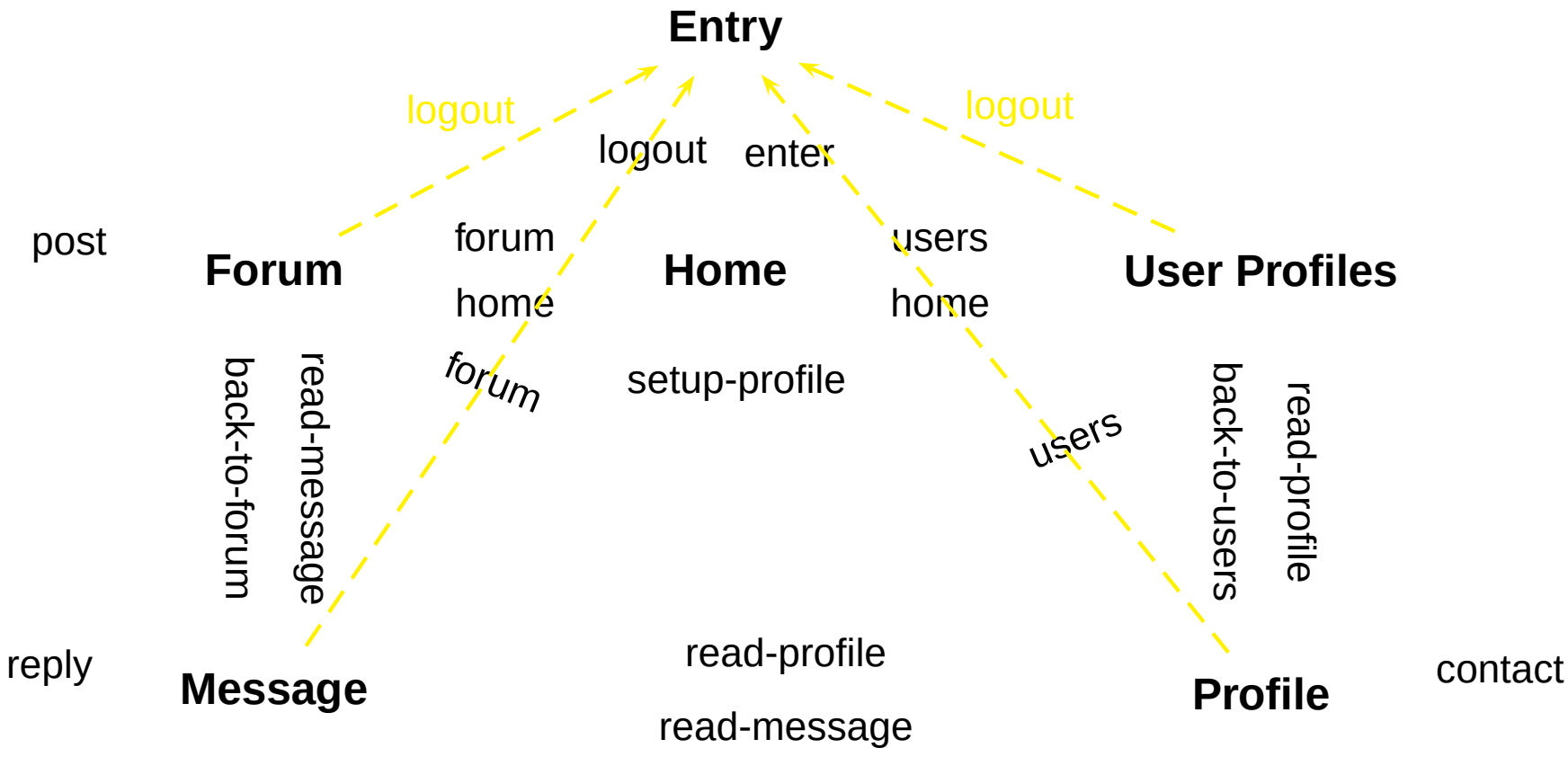
Web Interface 1



Web Interface 2



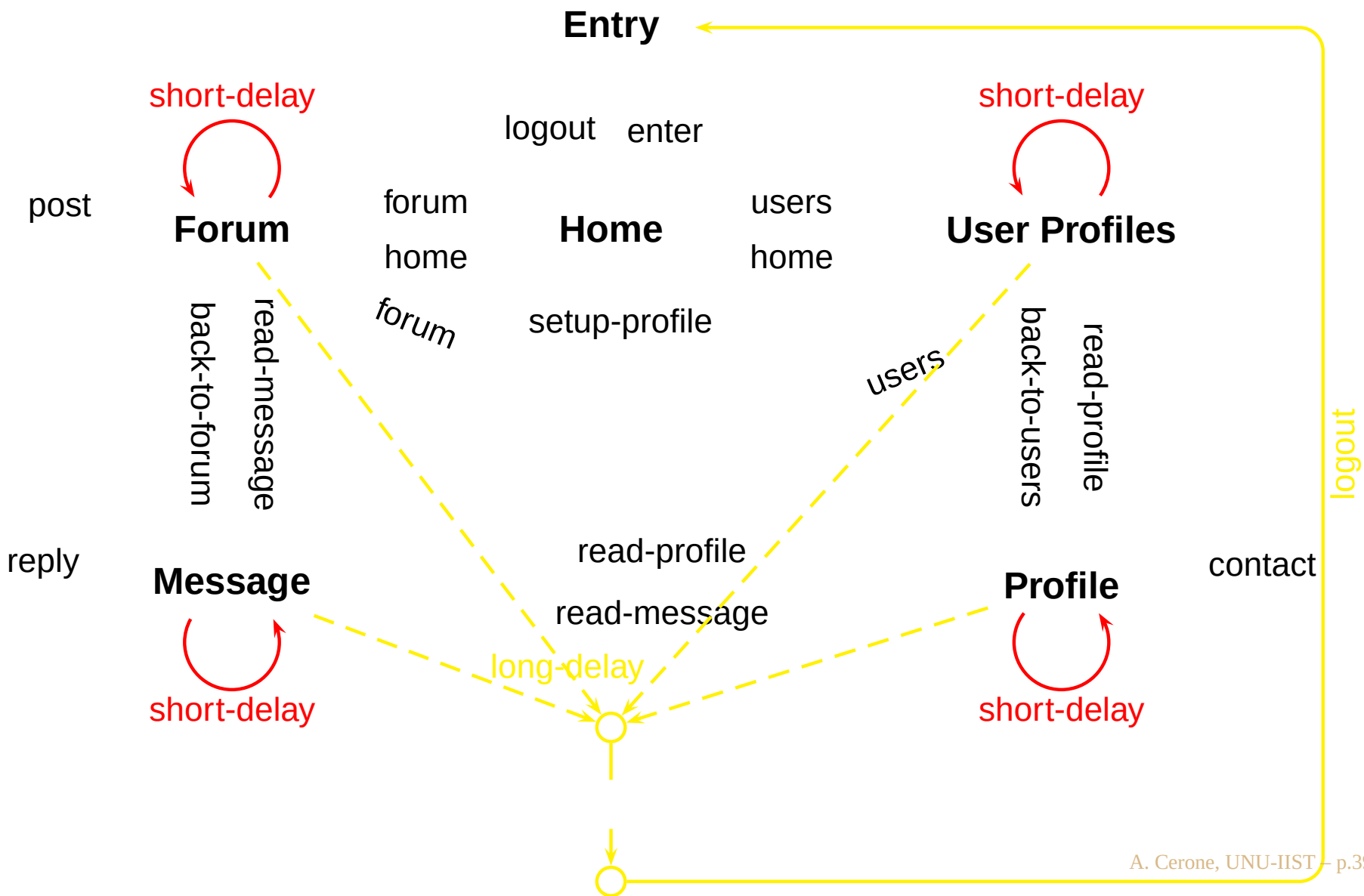
Web Interface 2



The property

- holds on ((**SYSTEM** || **NonExpert**) [| ... |] **NonForgetful**)
- does not hold on (**SYSTEM** || **NonExpert**)

Web Interface 3



Quick Timeout

Assumption: No authorised user may enter an unattended session within a time period shorter (short-delay) than the delay (long-delay) that triggers the timeout

Quick Timeout

Assumption: No authorised user may enter an unattended session within a time period shorter (short-delay) than the delay (long-delay) that triggers the timeout

back-to-forum
back-to-users
home
users
forum
logout

Quick Timeout

long-delay

timeout

logout

Quick Timeout

Assumption: No authorised user may enter an unattended session within a time period shorter (short-delay) than the delay (long-delay) that triggers the timeout

back-to-forum
back-to-users
home
users
forum
logout

Quick Timeout

long-delay

timeout

logout

The property

- holds on ((**SYSTEM** || **NonExpert**) [| ... short-delay ... |] **QuickTimeout**)
- does not hold on (**SYSTEM** || **NonExpert**)

Violation Prevention

Previous safeguards just reduce the likelihood of security violations

Violation Prevention

Previous safeguards just reduce the likelihood of security violations

Can we introduce a mechanism to prevent any unauthorised user entering an unattended session from performing interactions with the system?

Violation Prevention

Previous safeguards just reduce the likelihood of security violations

Can we introduce a mechanism to prevent any unauthorised user entering an unattended session from performing interactions with the system?

What about avoiding

- masquerading threats

Violation Prevention

Previous safeguards just reduce the likelihood of security violations

Can we introduce a mechanism to prevent any unauthorised user entering an unattended session from performing interactions with the system?

What about avoiding

- masquerading threats
- confidentiality threats

Violation Prevention

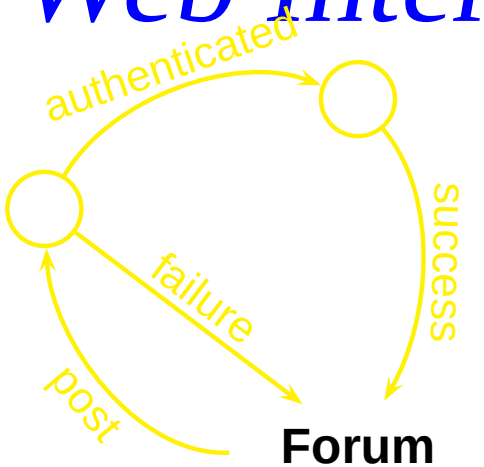
Previous safeguards just reduce the likelihood of security violations

Can we introduce a mechanism to prevent any unauthorised user entering an unattended session from performing interactions with the system?

What about avoiding

- masquerading threats
- confidentiality threats
- both masquerading and confidentiality threats

Web Interface 4



Entry

logout enter

Forum

forum
home

Home

forum
setup-profile

users
home

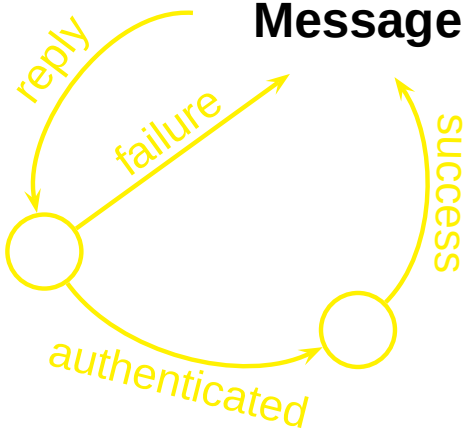
User Profiles

users
back-to-users
read-profile

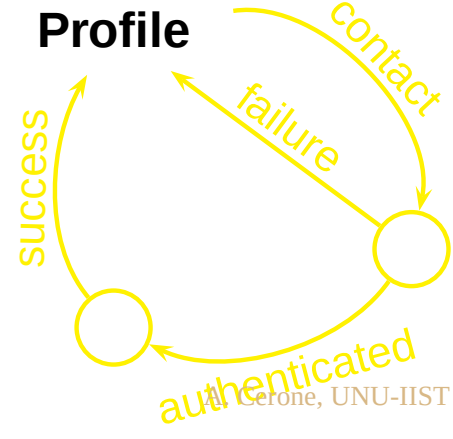
back-to-forum
read-message

read-profile
read-message

Message



Profile



More Security Properties

Does the previous property guarantee the absence of masquerading and/or confidentiality threats?

More Security Properties

Does the previous property guarantee the absence of masquerading and/or confidentiality threats? Yes!!

Does it hold on System 4?

More Security Properties

Does the previous property guarantee the absence of masquerading and/or confidentiality threats? Yes!!

Does it hold on System 4? No!

Why?

More Security Properties

Does the previous property guarantee the absence of masquerading and/or confidentiality threats? Yes!!

Does it hold on System 4? No!

Why? Too strong!

More Security Properties

Does the previous property guarantee the absence of masquerading and/or confidentiality threats? Yes!!

Does it hold on System 4? No!

Why? Too strong!

- masquerading prevention
  $\Box(\text{unattended} \rightarrow \neg\,(\text{set-up} \vee \text{contact} \vee \text{post} \vee \text{reply})\,\mathcal{W}\,\text{logout})$

More Security Properties

Does the previous property guarantee the absence of masquerading and/or confidentiality threats? Yes!!

Does it hold on System 4? No!

Why? Too strong!

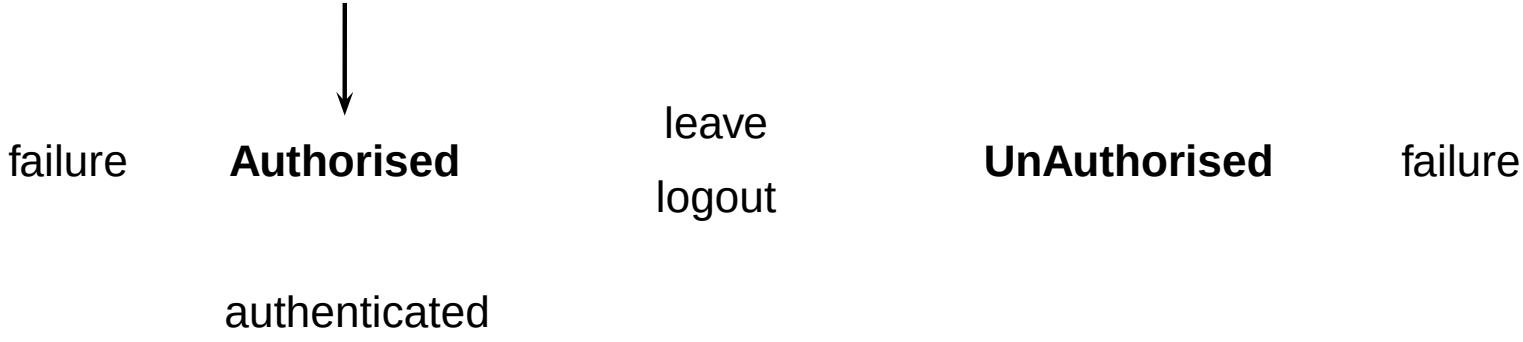
- masquerading prevention
  $\Box(\text{unattended} \rightarrow \neg\,(\text{set-up} \vee \text{contact} \vee \text{post} \vee \text{reply})\,\mathcal{W}\,\text{logout})$
- confidentiality
  $\Box(\text{unattended} \rightarrow \neg\,(\text{read-profile} \vee \text{read-message})\,\mathcal{W}\,\text{logout})$

Authentication

Assumption: Only authorised users can be authenticated

Authentication

Assumption: Only authorised users can be authenticated

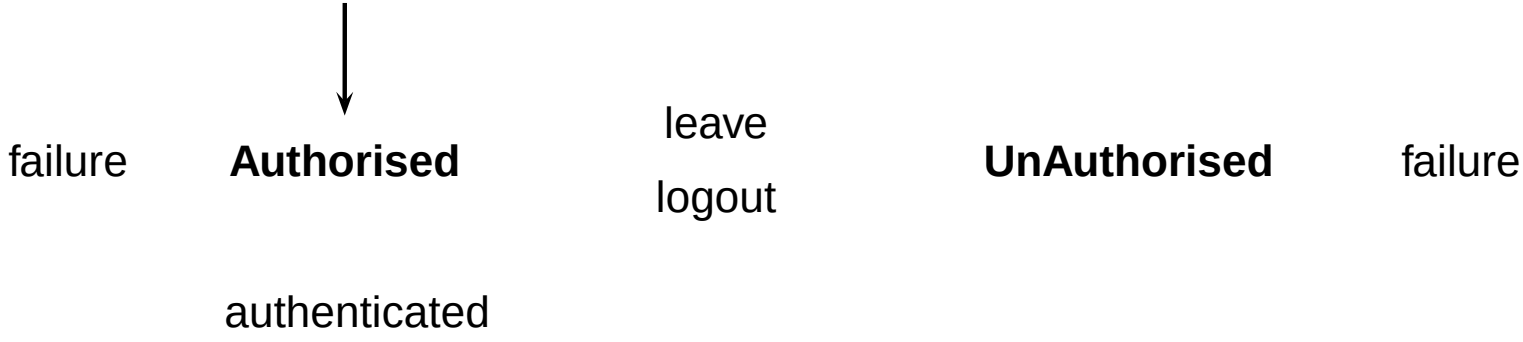


((**SYSTEM** $\|$ **NonExpert**) $\|$ **Authorised**)

- The following property holds
  $\Box(\text{achieved} \rightarrow \neg\text{success}\, \mathcal{U}\, (\text{goal} \vee \text{logout}))$

Authentication

Assumption: Only authorised users can be authenticated



((**SYSTEM** ‖ **NonExpert**) ‖ **Authorised**)

- If authentication is on `read-message` and `read-profile` then the following property holds

  $\Box(\text{unattended} \rightarrow \neg\,(\text{read-profile} \vee \text{read-message})\; \mathcal{W}\; \text{logout})$

Strong Property

	Expertise (*User*)	**NonForgetful** (*User*)	**Quick Timeout** (*Web Interface*)
Interface 1			
+ NonExpert	FALSE	FALSE	
+ Expert	FALSE	TRUE	
Interface 2 - logout			
+ NonExpert	FALSE	TRUE	
+ Expert	FALSE	TRUE	
Interface 3 - timeout			
+ NonExpert	FALSE		TRUE
+ Expert	FALSE		TRUE

Other Properties

	never-masquerading	*confidentiality*
Interface 4 - contact, post, reply	FALSE	FALSE
+ Authorised	TRUE	FALSE (!)
Interface 5 - read-message, read-profile	FALSE	FALSE
+ Authorised	FALSE (!)	TRUE
Interface 6 - *all above actions*	FALSE	FALSE
+ Authorised	TRUE	TRUE

$$\Box(\text{unattended} \rightarrow \neg\,(\text{set-up} \vee \text{contact} \vee \text{post} \vee \text{reply})\,\mathcal{W}\,\text{logout})$$

$$\Box(\text{unattended} \rightarrow \neg\,(\text{read-profile} \vee \text{read-message})\,\mathcal{W}\,\text{logout})$$

Intrusion

The user model is based that

- single user view
- only honest goals

Intrusion

The user model is based that

- single user view
- only honest goals

Cleaner approach

- intrusion goal (dishonest goal)

Intrusion

The user model is based that

- single user view
- only honest goals

Cleaner approach

- intrusion goal (dishonest goal)
  - masquerading goal
  - breaking confidentiality goal

Intrusion

The user model is based that

- single user view
- only honest goals

Cleaner approach

- intrusion goal (dishonest goal)
  - masquerading goal
  - breaking confidentiality goal
- environment process to describe the initial state as regular session or unattended session

Multiple Users

The user model is based that

- single user view
- only honest goals

Multiple Users

The user model is based that

- single user view
- only honest goals

Cleaner approach

- several user

Multiple Users

The user model is based that

- single user view
- only honest goals

Cleaner approach

- several user
  - maybe partitioned in honest and dishonest

Multiple Users

The user model is based that

- single user view
- only honest goals

Cleaner approach

- several user
  - maybe partitioned in honest and dishonest
- no need of environment process

References

[Cranor and Garfinkel 05]

Lorrie Faith Cranor and Simson Garfinkel (eds.).
Security and Usability — Designing Secure systems That People Can Use.
O'Really, 2005.

Edited Book

Collection of 34 essays from leading security and human-computer interaction researchers aiming at usable security.

[Cerone and Elgegbyan 07]

A. Cerone and N. Elgegbyan.
Model-checking Driven Design of Interactive Systems.
ENTCS 183, Elsevier, 2007, pages 3–20.

Formal Methods Paper
Use of model-checking to improve the interface design with respect to security properties.

End