Privacy Arguments

Managing Selective Disclosure Requirements in Mobile Applications

1 Mobile privacy is dependent on user context





2 Privacy norms guide what to share with whom and when

"It is acceptable to share location information with colleagues during work hours."

"It is not OK to find location of colleagues when they are away on holiday."

"It is not customary to share location information of colleagues with friends at any time."

3 Privacy needs are also specific to individual users

"Bob does not want to share his location information with Sarah on Thursdays and Fridays."

"Alice does mind sharing her location information with her colleague Carole during her holiday."

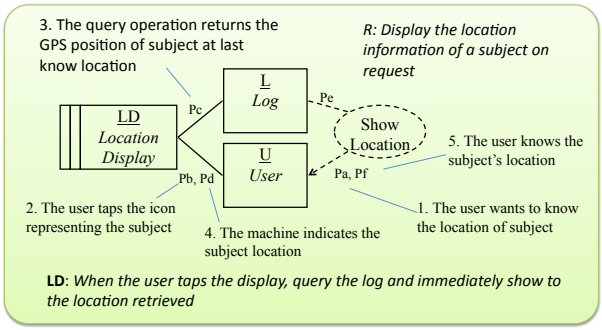
"Alice does mind sharing her location information with her colleague Carole during her holiday."

4 New challenges for Requirements Engineering

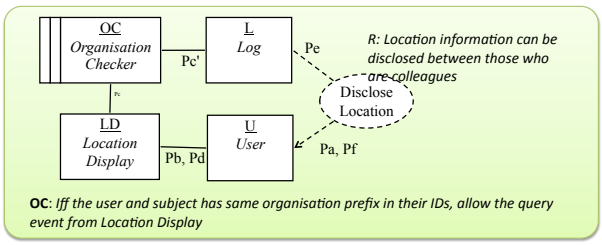
Representation of requirements for individual and classes of users

Formal reasoning about requirements for privacy

5 Privacy Argument captures a class of software behaviour and its context satisfying privacy requirements



A *problem diagram* describes software behavior, context, requirement and their relationship.



A *transformed* problem diagram describes the architecture for enforcing the privacy in the original problem diagram.

```
argument: Colleague_Norm_Class
A1 "<<User>> can find out location
information of his/her colleague
<<subject>>" {
  supported by
    F2 "<<User>> taps the screen icon of
<<subject>>"
  warranted by
    R1 "If <<user>> taps the screen, the
machine checks whether <<user>> and
<<subject>> are colleagues"
    R2 "If <<user>> and <<subject>> are
colleagues, the machine queries the
location of <<subject>>"
…
}
```

A *privacy argument class* show why privacy requirements will be satisfied by the software in a particular context.

```
A4 "Bob prefers to share with colleagues on
weekdays and with friends on weekends" {
 preferred by
   A2 precedes A3
     when (day >= Monday & day <= Friday)
   A3 precedes A2
     when (day >= Saturday & day <= Sunday)
}
```

Individual users such as *Bob* can specify individual preference and exceptions to norms.

6 Reference

T.T. Tun, A.K. Bandara, B.A. Price, Y. Yu, C. Haley, I. Omoronyia and B. Nuseibeh (2012) *Privacy Arguments: Analysing Selective Disclosure Requirements for Mobile Applications*. In: 20th IEEE International Requirements Engineering Conference, 24-28 September 2012, Chicago, Illinois.