Normative Requirements and Refinement

Özgür Kafalı

We outline an approach to capture natural language requirements as social norms. We review the background on norms and requirements, and use examples to illustrate the connection between them.

Social Norms

Humans, organizations and technical systems such as software interplay with each other in a *sociotechnical* system (STS). To capture the requirements of an STS, we adopt Singh's [2] model of norms. A norm is directed from a subject to an object and is constructed as a conditional relationship involving an antecedent (which brings the norm in force) and a consequent (which brings the norm to satisfaction). This representation yields clarity on who is accountable to whom. A norm has four core elements—SUBJECT, OBJECT, antecedent, and consequent. It can be formalized as $\mathsf{N}(\text{SUBJECT}, \text{OBJECT}, \mathit{antecedent}, \mathit{consequent})$.

Norms in our approach are of the following main types.

A commitment means that its subject commits to its object to ensure the consequent if the antecedent holds. For example, in a hospital, physicians are committed to the hospital to operating upon patients when there is an emergency. We write this commitment as:

$\mathsf{C}(\text{PHYSICIAN}, \text{HOSPITAL}, \mathit{emergency}, \mathit{operate})$

An authorization means that its subject is authorized by its object for bringing about the consequent if the antecedent holds. For example, physicians are authorized by the patients to access their electronic health record (EHR) if the patients give consent. We write this authorization as:

$\mathsf{A}(\text{PHYSICIAN}, \text{PATIENT}, \mathit{consent}, \mathit{access\_EHR})$

A prohibition means that its subject is forbidden by its object from bringing about the consequent if the antecedent holds. For example, health care professionals (HCP) are prohibited by the hospital from disclosing patients' protected health information (PHI). We write this prohibition as (true in the antecedent means that the norm is unconditional):

$\mathsf{P}(\text{HCP}, \text{HOSPITAL}, \mathit{true}, \mathit{disclose\_PHI})$

Requirements

Requirements represent what the stakeholders expect from an STS, and are usually expressed in natural language. Consider the following scenario.

Medical emergency scenario: There has been a public emergency near the hospital, and several unconscious patients need to be operated upon immediately. The hospital does not have the required number of physicians on staff to attend to the emergency situation. Therefore, it has to call in volunteer physicians from nearby hospitals. The volunteer physicians must not disclose the patients' PHI.

There are three requirements associated with the above scenario.

R-Operate Physicians must operate upon patients immediately when there is a medical emergency. We can capture this requirement with the following commitment:

$\mathsf{C}(\text{PHYSICIAN}, \text{HOSPITAL}, \mathit{emergency}, \mathit{operate})$

R-Help The hospital may allow volunteer physicians from other hospitals to help with the treatment of patients. We can capture this requirement with the following authorization:

$\mathsf{A}(\text{VOLUNTEER}, \text{HOSPITAL}, \mathit{emergency}, \mathit{treat})$

R-Disclose Volunteer physicians must not disclose the patients' PHI. We can capture this requirement with the following prohibition:

$\mathsf{P}(\text{VOLUNTEER}, \text{HOSPITAL}, \mathit{true}, \mathit{disclose\_PHI})$

Refinement

Norm specifications can initially be broad. That is, they may not cover specific situations that might lead to opportunities being missed, and eventually cause the violation of some of the requirements. When this is the case, the stakeholders should refine the norms to account for the situation at hand. This is similar to classical refinement, i.e., weakening or strengthening of preconditions or postconditions [1]. Norm refinement can be performed by applying logic operators (NOT, AND, OR) on the propositions of norms (antecedent, consequent). Consider the following authorization:

$\mathsf{A}(\text{PHYSICIAN}, \text{HOSPITAL}, \mathit{consent}, \mathit{access\_EHR})$: the physician is authorized by the hospital to access patients' EHR provided there is consent.

One refinement of the authorization is the following:

$\mathsf{A}(\text{PHYSICIAN}, \text{HOSPITAL}, \mathit{consent}\ \text{OR}\ \mathit{emergency}, \mathit{access\_EHR})$: the physician is authorized to access patients' EHR provided there is consent or when there is an emergency (i.e., the precondition is weakened).

References

[1] K. Pohl. The three dimensions of requirements engineering: A framework and its applications. *Information Systems*, 19(3):243–258, Apr. 1994.

[2] Munindar P. Singh. Norms as a basis for governing sociotechnical systems. *ACM Trans. Intell. Syst. Technol.*, 5(1):21:1–21:23, December 2013.