CSC 495.002 – Homework#3: Extracting Privacy Requirements and Norms

Dr. Özgür Kafalı
North Carolina State University
Department of Computer Science

For each of the three scenarios described below, first extract the natural language requirements from the scenario and then specify the necessary norms to satisfy the requirements.

The deadline for this assignment is October 4th – 5PM.

Sample solution:

Consider the following scenario from a medical emergency:

"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. However, the volunteer physicians are not supposed to disclose the patients' protected health information (PHI)."

There are three requirements associated with the above scenario.

R-Operate Physicians must operate upon patients immediately when there is a medical emergency.

R-Help The hospital may allow volunteer physicians from other hospitals to help with the treatment of patients.

R-Disclose Volunteer physicians must not disclose the patients' PHI.

We can capture the above requirements with the following norms. Note that the number of norms may not necessarily be equal to the number of requirements. However, in this case, we need three norms to capture the above requirements.

C(PHYSICIAN, HOSPITAL, emergency, operate)

A(VOLUNTEER, HOSPITAL, emergency, treat)

Pro(VOLUNTEER, HOSPITAL, true, disclose_PHI)

Scenario 1: Health Care Privacy Scenario

Consider a health care scenario involving the privacy of patient's protected health information [HHS, 2003]:

"Hospitals are bound by law to keep their patient's electronic health records (EHR) private. Therefore, when a patient is admitted to a hospital, the physician treating the patient must not publish the patient's protected health information (PHI) online. However, the physician may share the patient's PHI with a colleague to get an expert opinion. Moreover, the physician may share the patient's PHI with the patient's family when there is an emergency."

Specify the requirements in natural language. For norms, use the following users and propositions in your specification. Note that not all of them might be applicable.

Users: PHYSICIAN, PATIENT, HOSPITAL

Propositions: true, emergency, patient_visit, access_ehr, publish_phi_online, share_phi_colleague, share_phi_family

Scenario 2: Health Care Security Scenario

Consider a health care scenario involving the security of patient's electronic health records (EHR) [HHS, 2003]:

"Hospitals are bound by law to keep their patient's electronic health records (EHR) secure. Therefore, health care workers who have access to patients' EHR must not share their credentials (username and password) with anyone. If health care workers need to use a public computer (such as the computer in the emergency department), they must log off from the computer as soon as they are finished reviewing the patient's EHR. Moreover, health care workers must not view the EHR of their friends unless they are responsible for their treatment."

Specify the requirements in natural language. For norms, use the following users and propositions in your specification. Note that not all of them might be applicable.

Users: WORKER, PHYSICIAN, PATIENT, HOSPITAL

Propositions: true, emergency, share_id, share_password, access_ehr, public_computer, logout, friend, treating

Scenario 3: Academic Access Control Scenario

Consider an access control scenario for an academic building involving the confidentiality and integrity of its sensitive resources [Tsigkanos et al., 2014].

"An academic department has a number of functions to keep running. Exams are kept in the department's safe room. Professors have access to the safe room. Teaching assistants may access exams, however they must not be in the safe room when the professor is present to keep the safe's security code confidential. Exams are printed using the departmental printer. When there is a problem, a technician is called to repair the printer. A visiting technician is allowed to enter the printer room. In general, visitors are only allowed in public areas and rooms they are supposed to carry out work. Often, grad students need training on the department's server. However, they are not allowed to enter the server room when authorized staff are not present to preserve the integrity of the server."

Specify the requirements in natural language. For norms, use the following users and propositions in your specification. Note that not all of them might be applicable.

Users: TECHNICIAN, GRADUATE_STUDENT, TEACHING_ASSISTANT, PROFESSOR, SECURITY_ADMIN

Propositions: true, printer_broken, access_printer, access_server, access_safe, access_public_area, exam_period, staff_present, professor_present

References

[HHS, 2003] HHS (2003). Summary of the HIPAA privacy rule. United States Department of Health and Human Services (HHS). http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/.

[Tsigkanos et al., 2014] Tsigkanos, C., Pasquale, L., Menghi, C., Ghezzi, C., and Nuseibeh, B. (2014). Engineering topology aware adaptive security: Preventing requirements violations at runtime. In *Proceedings of the 22nd IEEE International Requirements Engineering Conference (RE)*, pages 203–212.