Academic Access Control Scenario

Özgür Kafalı

Consider an access control scenario for an academic building involving the confidentiality and integrity of its sensitive resources [1].

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.

Agents

TECHNICIAN, GRADUATE_STUDENT, TEACHING_ASSISTANT, PROFESSOR, SECURITY_ADMIN

Propositions

$true, printer\_broken, access\_printer, access\_server, access\_safe,$
$access\_public\_area, exam\_period, staff\_present, professor\_present$

Deliverables

- Identify the natural language requirements for the scenario
- Refine the following norms using the above agents and propositions to satisfy the identified requirements for the scenario

$\mathsf{A}(\text{TECHNICIAN}, \text{SECURITY\_ADMIN}, printer\_broken, access\_printer)$
$\mathsf{P}(\text{GRADUATE\_STUDENT}, \text{SECURITY\_ADMIN}, true, access\_server)$

$\mathsf{A}(\text{PROFESSOR}, \text{SECURITY\_ADMIN}, true, access\_safe)$
$\mathsf{P}(\text{TEACHING\_ASSISTANT}, \text{SECURITY\_ADMIN}, true, access\_safe)$

References

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