

[0047] usr is the actual identity of the user who is acting as the role (here, of HNurse);

[0048] !=is not equal; and

[0049] && is a logical AND.

[0050] The above expression specifies that only when the expression within [[]] evaluates to true, can the user with the HNurse role view the object O.

Example 2

[0051] Medical researchers can only view records of patients who have taken some medicines that are the subject of the researchers' study.

[0052] For this constraint, determining user access within the role's permission requires extensive knowledge about the record's content, i.e., medicines, and information about the individual user (subject) and the user's studies (likely to be environmental content stored outside the controlled computer system). A parenthetical category review of Example 2 shows: Medical researchers (role) can only (constraint) view (operations) records of patients (object) who have taken some medicines (object content) that are the subject of the researchers' (subject content) study (environment content).

[0053] Therefore, when:

[0054] Patient-Record: O

[0055] Roles: R={Researcher}

[0056] Operations: OP={view, append, copy}

[0057] Application Context:

[0058] Relationship: rcr=Role-RecordContent Relationship;

in a formal specification, the role-Permission Assignment with Context Constraints may be written as following:

[0059] PA (Researcher, O, view) [[rcr(usr(Researcher), medicine-content(O))]].

[0060] The above expression specifies that only when the expression within [[]] evaluates to true, can the user with the Researcher role view the object O, where usr is defined as in Example 1.

Example 3

[0061] Medical researchers can only view records of patients who exhibit similar symptoms as those exhibited by patients who suffer from the SARS Disease.

[0062] For this constraint, determining user access requires external access to databases that describe symptoms for the SARS disease. A parenthetical category review of Example 3 shows: Medical researchers (role) can only (constraint) view (operation) records of patients (object) who exhibit similar symptoms (object content) as those exhibited by patients who suffer from the SARS Disease (environment content).

[0063] Therefore, when:

[0064] Patient-Record: O

[0065] Roles: R={Researcher}

[0066] Operations: OP={view, append, copy}

[0067] Application Context:

[0068] Relationship:

[0069] rcr=Role-RecordContent Relationship

[0070] sr=similarity relationship;

in a formal specification, the role-Permission Assignment with Context Constraints may be written as:

[0071] PA(Researcher, O, view) [[rcr(Researcher, symptom-content(O)) && sr(symptom-content(O), symptoms(SARS))]].

[0072] The above expression specifies that only when the expression within [[]] evaluates to true, can the user with the Researcher role view the object O.

Example 4

[0073] Pediatricians are allowed to view their patients' parents' blood-test results, but only that part of the parental records.

[0074] For this constraint, determining user access requires extensive knowledge about record content and the context determination of complex relationships. A parenthetical category review of Example 4 shows: Pediatricians (role) are allowed to view their patients' parent (could be either of subject context derived from the patient identity or object content based on patient record contents) blood-test results (object content), but only (constraint) that part of the parental records.

[0075] Therefore, when:

[0076] User: U

[0077] Patient-Record: O

[0078] Roles: R={Pediatrician}

[0079] Operations: OP={view, append, copy}

[0080] Application Context:

[0081] Relationship:

[0082] pd=patient-doctor relationship

[0083] pc=parent-child relationship

[0084] rcr=role-content relationship;

in a formal specification, the role-Permission Assignment with Context Constraints may be written:

[0085] PA (Pediatrician, O, view) [[pd(child(owner(O)), usr(Pediatrician)) && rcr (Pediatrician, blood-content(O))]].

[0086] The above expression specifies that only when the expression within [[]] evaluates to true, can the user with the Pediatrician role view the object I.

Example 5

[0087] Records that have not been accessed within the last 5 years are not allowed to be accessed by doctors.

[0088] For this constraint, such as in a situation requiring the determination of a patient's medication, determining user access requires knowledge about the record's accessing