
MODULE *AccessControlManagement*

EXTENDS *Naturals, Sequences*

CONSTANTS *Apps, Perms*

$NULL \triangleq \text{"NULL"}$

$ALLOW \triangleq \text{"ALLOW"}$

$REJECT \triangleq \text{"REJECT"}$

$Boolean \triangleq \{\text{TRUE}, \text{FALSE}\}$

$Consent \triangleq \{ALLOW, REJECT\}$

VARIABLE *ACL, Resource*

$TypeOK \triangleq \bigwedge \forall a \in Apps : \forall p \in Perms : \bigwedge ACL[a][p] \in Consent \cup \{NULL\}$
 $\quad \quad \quad \bigwedge Resource[a][p] \in Boolean$

$decide(a, p) \triangleq \bigwedge \exists c \in Consent :$
 $\quad \quad \quad ACL' = [ACL \text{ EXCEPT } ![a] = [ACL[a] \text{ EXCEPT } ![p] = c]]$

$use(a, p) \triangleq \bigwedge ACL[a][p] = ALLOW$
 $\quad \quad \quad \bigwedge Resource' = [Resource \text{ EXCEPT } ![a] = [Resource[a] \text{ EXCEPT } ![p] = \text{TRUE}]]$
 $\quad \quad \quad \bigwedge \text{UNCHANGED } \langle ACL \rangle$

$ask(a, p) \triangleq \text{IF } ACL[a][p] = NULL$
 $\quad \quad \quad \text{THEN } \bigwedge decide(a, p)$
 $\quad \quad \quad \quad \quad \bigwedge \text{UNCHANGED } \langle Resource \rangle$
 $\quad \quad \quad \text{ELSE}$
 $\quad \quad \quad \quad \quad \bigwedge \text{UNCHANGED } \langle ACL, Resource \rangle$

$Init \triangleq \bigwedge ACL = [a \in Apps \mapsto [p \in Perms \mapsto NULL]]$
 $\quad \quad \quad \bigwedge Resource = [a \in Apps \mapsto [p \in Perms \mapsto \text{FALSE}]]$

$Next \triangleq \bigvee \exists a \in Apps : \exists p \in Perms : \bigvee ask(a, p)$
 $\quad \quad \quad \quad \quad \bigvee use(a, p)$

$vars \triangleq \langle ACL, Resource \rangle$

$Authorized \triangleq \Box \neg (\bigwedge \exists a \in Apps : \exists p \in Perms :$
 $\quad \quad \quad \bigwedge Resource[a][p] = \text{TRUE}$
 $\quad \quad \quad \bigwedge ACL[a][p] \neq ALLOW)$

$Spec \triangleq Init \wedge \Box [Next]_{vars} \wedge Authorized$

\ * Modification History

\ * Last modified *Thu Mar 23 14:10:47 GMT+03:30 2023 by Amirhosein*

\ * Created *Thu Mar 23 07:45:26 GMT+03:30 2023 by Amirhosein*