

## Modèle de contrôle d'accès et politiques de sécurité pour les grandes infrastructures critiques

*Yves DESWARTE*

Les grandes infrastructures critiques d'approvisionnement, de transport ou de services se caractérisent par les conséquences potentiellement dramatiques de leurs défaillances. Ces défaillances peuvent être dues à des pannes physiques ou logiques de composants, ou à des interactions incorrectes à l'intérieur d'une infrastructure ou entre infrastructures interdépendantes. Le réseau de production, de transport et de distribution d'énergie électrique est l'une des plus critiques de ces infrastructures car elle interagit avec toutes les autres. Elle est aussi l'une des plus vulnérables et des plus complexes, car elle met en jeu une grande variété d'acteurs, depuis des compagnies internationales jusqu'à des particuliers, avec une extension géographique à l'échelle de continents entiers. Elle est donc particulièrement susceptible d'être la cible de terroristes. De plus, la dérégulation du secteur au niveau européen, une concurrence sévère entre les compagnies et des enjeux financiers importants font que les différentes parties prenantes sont amenées à coopérer dans un climat de méfiance mutuelle.

Il est donc primordial d'assurer la sécurité des systèmes d'information qui soutiennent cette infrastructure critique, puisque les malveillances ne sont pas exclues et qu'elles peuvent avoir des conséquences catastrophiques. Or les modèles de sécurité classiques s'accommodent mal de la complexité des organisations et, faute d'une autorité centrale reconnue par tous, il serait illusoire de vouloir imposer une politique de sécurité commune à toutes les organisations participant à cette infrastructure. Il faut dès lors développer un modèle et des politiques de sécurité de façon à favoriser les interactions entre ces organisations, tout en garantissant la sécurité et l'autonomie de chacune d'elles.

Le modèle PolyOrBAC que nous avons développé permet à chaque organisation de gérer sa propre politique de sécurité indépendamment des autres, d'assurer la protection de ses biens par ses propres mécanismes de sécurité et d'exercer sa responsabilité, en particulier vis-à-vis de ses propres utilisateurs. Ce modèle favorise aussi les interactions entre organisations, sous forme de services Web. Ce modèle est soutenu par des extensions au modèle de contrôle d'accès basé sur les organisations (le modèle OrBAC), permettant d'exprimer les politiques de sécurité locales à chaque organisation, et par une notion nouvelle de politique-contrat, établie entre chaque organisation fournissant un service Web et chaque organisation qui utilise ce service. Cette politique-contrat est vérifiée en temps-réel à chaque interaction entre organisations, et elle permet de détecter les erreurs ou les abus de l'une ou l'autre, et de présenter les preuves de ces abus ou erreurs à une tierce partie de confiance qui peut imposer des pénalités à l'organisation responsable.