Contrôle d'inférence non-autorisée basé sur la logique floue dans les systèmes d'information et de communication en santé et en social

Souhila Kaci[1], Abdeslam Ali-Laouar[2], Frédéric Cuppens[2]
[1] Centre de Recherche en Informatique de Lens (C.R.I.L.)–C.N.R.S.
Université d'Artois, Rue Jean Souvraz SP 18 62307 Lens Cedex, France
[2] Institut de Recherche en Informatique de Toulouse (I.R.I.T.)–C.N.R.S.
Université Paul Sabatier, 118 route de Narbonne 31062 Toulouse Cedex 4, France

L'objectif des travaux sur les modèles et politiques de sécurité pour les systèmes d'information et de communication en santé et en social consiste à définir et spécifier les propriétés de sécurité du secteur socio-sanitaire, et d'élaborer et de développer un modèle de politique de sécurité. Il repose sur les notions classiques de la sécurité des systèmes d'information, utilisant les concepts spécifiques aux systèmes d'information et de communication en santé et en social. Notons cependant que malgré la mise en œuvre de politiques de sécurité dédiées, il est toujours possible pour un attaquant externe et, surtout, pour un utilisateur interne mal intentionné, d'essayer de contourner les mécanismes de contrôle d'accès aux ressources mises en œuvre afin de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des services et des données.
Pour empêcher les infractions contre l'intimité des patients, les bases de données médicales doivent protéger non seulement des informations confidentielles, mais également des informations non explicitement confidentielles qui peuvent être employées pour obtenir des informations confidentielles. Une solution possible à ce problème est de refuser de répondre lorsque la réponse risque de permettre d'inférer une information confidentielle. Une autre solution possible est de fournir des réponses fausses aux utilisateurs ayant un accès restreint au système d'information. En employant cette méthode, on peut protéger des informations confidentielles en fournissant des réponses fausses mais peu sensibles. Le problème de cette méthode est qu'il n'est pas toujours facile de fournir un ensemble cohérent de fausses réponses. La solution que nous avons proposée pour faire face à l'inférence d'informations confidentielles consiste non pas à fournir une réponse fausse à l'utilisateur mais plutôt une réponse "vague" en utilisant pour cela la *logique floue*. Informellement, cela revient à dire que l'on remplace chaque réponse numérique (par exemple, le nombre de patients=1) par une réponse vague (par exemple "peu"). Nous avons étudié différentes possibilités d'atteintes de la confidentialité du système et avons montré que notre solution permet à chaque fois de faire face à l'attaque.