

СЕМАНТИЧЕСКАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бен Кафо Али Ахмед Саид

Саломатин С. Б. – к.т.н., доцент

Развитие современных инфокоммуникационных сети, направлено на автоматизацию, интеграцию и повторное использование данных в различных веб-приложениях. Это предъявляет новые требования к механизмам безопасности, особенно в моделях управления доступом. Доступ к ресурсам может контролироваться безопасным способом, если решение о доступе учитывает семантические отношения между объектами в моделях данных сети.

Контроль доступа - это механизм, который позволяет владельцам ресурсов определять, управлять и обеспечивать соблюдение условий доступа, применимых к каждому ресурсу [1-3]. Механизм контроля доступа с учетом семантики должен гарантировать, что только правомочные пользователи имеют право на получение права доступа, и каждый правомочный пользователь должен иметь возможность доступа ко всем ресурсам, на которые он / она авторизован [4].

Традиционные модели управления доступом, такие как MAC, DAC и RBAC, не решают эту проблему, поскольку они не учитывают многообразие семантических отношений в моделях данных.

Семантическая модель управления доступом (SBAC) в процессе принятия решений рассматривает семантические отношения между различными объектами в субъектных, предметных областях и в области действий.

Принятие решений на основе изолированных объектов при игнорировании семантических взаимосвязей между ними может привести к незаконным доступам неавторизованных пользователей и неполному предоставлению прав доступа.

Рассмотрим семантическую модель управления доступом (SBAC), которая аутентифицирует пользователей на основе их учетных данных, предоставляемых в процессе запроса на право доступа.

Положим, что SBAC принимает решения по трем областям: предмет, объект и действие и состоит из трех основных компонентов: базы онтологий, базы авторизации и операций. База онтологий - это набор онтологий: предметная онтология (SO), объектная онтология (OO) и онтология действия(АО).

Объектная онтология. Объекты - это сущности, к которым осуществляется доступ и / или изменения. Объект принадлежит объектной онтологии, которая показывает структуру, в которой объекты (концепции, индивидуумы и свойства) организованы вместе с семантическими отношениями между ними.

Предметная онтология. Субъекты являются активными субъектами требующим доступа к объектам. Субъектами являются понятия или отдельные лица в предметной онтологии. Представление учетных данных определяет право пользователей на доступ к ресурсу.

Антология действия. АО зависит от типа действий, которые субъекты стремятся выполнить над объектом. Каждый тип действия является концепцией в онтологии, а действия являются индивидуумами концепции, определенной в АО.

Моделируя домены управления доступом с использованием онтологий, SBAC стремится учитывать семантические отношения на разных уровнях онтологии при принятии решения о запросе доступа. При этом используется база авторизации - набор правил авторизации в форме (s, o, ± a), в которых s - это объект в SO, o - это объект, определенный в OO, и a - это действие, определенное в АО. Поскольку SBAC работает на основе логического вывода для предотвращения распространения одного и того же решения (предоставить / запретить) на все выведенные правила, он позволяет определять правила исключения с более высоким приоритетом.

SBAC может быть использована как модель управления доступом для защиты ресурсов SemanticWeb. SBAC учитывает семантические взаимосвязи между объектами в областях принятия решений по управлению доступом. Автоматическое принятие решений в SBAC о предоставлении или отклонении запроса на доступ осуществляется через процессы логического вывода на основе семантического отношения между объектами.

Список использованных источников:

1. Hengartner, U., Steenkiste, P.: Exploiting information relationships for access control. In: proceeding of third IEEE International Conference on Pervasive Computing and Communications, Percom 2005, Kauai, Island HI (2005) 278–296
2. Bonatti, P.A., Duma, C., Fuchs, N., Nejdi, W., Olmedila, D., Peer, J., Shahmehri, N.: Semantic web policies – a discussion of requirements and research issues. In:ESWC 2006. (2006) 712–724
3. Samarati, P., di Vimercati, S.C.: Access control: Policies, models, architectures. In:FOSAD 2000. Volume 2171 of LNCS., Springer-Verlag (2001) 137–196
4. Qin, L., Atluri, V.: Concept-level access control for the semantic web. In: ACM Workshop on XML Security, Fairfax, VA, USA (2003) 94–103