УДК 004.056

С.Г. Семенов

Національний технічний університет «Харківський політехнічний інститут», Харків

КОНЦЕПЦІЯ ВДОСКОНАЛЕНОЇ ТЕХНОЛОГІЇ ОПИСУ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ ДЛЯ ЗАХИСТУ ДАНИХ В КОМП'ЮТЕРНІЙ СИСТЕМІ

Проведено аналіз технологій опису моделей розмежування доступу до ресурсів комп'ютерних систем. Визначено, що однією з перспективних мов моделювання є мова XACML. Визначено основні її недоліки і запропонована концепція, що дозволяє врахувати фактор післядії в процесі моделювання розмежування доступу до ресурсів. Удосконалена модель потоків даних при розмежуванні доступу до комп'ютерної системи. Запропоновані рекомендації щодо практичного використання. Зроблено висновок про можливість зменшення часу на дозвіл запиту на доступ до комп'ютерної системи.

Ключові слова: *захист даних, розмежування доступу, технології опису моделей, мова XACML.*

Постановка проблеми і аналіз літератури

На теперешній час у зв'язку з інтенсивним зростанням потреби в обчислювальних і телекомунікаційних системах, розвитком комп'ютерної техніки і збільшенням числа користувачів, все більша увага приділяється питанням контролю доступу до їх ресурсів. Подібний контроль реалізується через задані адміністратором обмеження доступу, тобто, можливості виконати певні дії, користувачів по відношенню до ресурсів системи. Для цього в певної математичної моделі задається формальний, суворо певний набір правил. Ці правила, як правило, записуються на деякій мові.

У ряді нормативних документів [2, 4], що регламентують питання захисту інформаційної безпеки, визначено вимоги до розроблюваних систем захисту даних. Одною з цих вимог є наявність форм технологічного моделювання процесів розмежування доступу. У той же час багатокомпонентність програмної та апаратної складових комп'ютерної системи, гетерогенність засобів взаємодії в значній мірі ускладнює процес формального опису зазначених вище технологій і стимулює розробників до створення нових логіко-мовних засобів опису технологій розмежування доступу [1, 5, 6].

Проведений аналіз літератури [1, 3] показав, що одним з таких рішень є мова розмітки контролю доступу XACML, який має можливості:

– комбінування окремих правил і політик в одну множину політик, яка застосовуватиметься при кожному запиті доступу;

– вибору декількох способів комбінування правил і політик;

– визначення атрибутів для різних елементів правил;

– надання множини логічних і математичних операторів над атрибутами суб'єкта, ресурсу та оточення.

Одним з ключових понять, на основі якого формулюються моделі в стандарті XACML, є поняття атрибута. Атрибутом є властивість суб'єкта, об'єкта, типу доступу або оточення. Кожен атрибут має ім'я і фіксований тип даних, які можуть в ньому міститися. Розмежування доступу проводиться на основі значень атрибутів суб'єкта, об'єкта, типу доступу і середовища оточення, які враховуються при ухваленні рішення про доступ.

Мова XACML надає широкий спектр засобів для опису технології розмежування доступу. Разом з тим, вона має суттєві недоліки, які ускладнюють як теоретичні дослідження цієї мови, так і практичну реалізацію механізмів розмежування доступу, створених на її основі. Одним з найважливіших недоліків мови є її складність, як чисто синтаксична, так і складність опису семантики. Синтаксична складність проявляється в тому, що запис навіть простих моделей розмежування доступу за допомогою XACML надмірно довгий і погано сприймається користувачем. Семантична складність полягає у великій кількості понять, які визначаються в стандарті мови. Ця обставина ускладнює розробку формальної моделі мови в цілому.

Крім цього, одним з основних недоліків розглянутої мови є відсутність обліку фактора післядії в системі. Тому актуальною науковою задачею є удосконалення технологи опису моделей розмежування доступу до ресурсів комп'ютерної системи.

Розвиток технології опису моделей розмежування доступу

Проведені дослідження показали, що основним поняттям, на якому базуються моделі логічного розмежування доступу, що описуються з використанням мови XACML, крім понять суб'єкта, об'єкта і типу доступу, є поняття атрибуту безпеки. Кожен об'єкт, суб'єкт, тип доступу, а також оточення може мати деякі запрограмовані користувачем або механізмом логічного розмежування доступу атрибути безпеки.

Модель розмежування доступу формулюється у вигляді деяких умов на атрибути безпеки суб'єкта, об'єкта, типу доступу та оточення.

Будь-який запит доступу користувача до ресурсу повинен перериватися системної сутністю PEP (Policy Enforcement Point). При цьому PEP створює запит в форматі XACML і посилає його системної сутності PDP (Policy Decision Point). Policy Decision Point (PDP) – системна сутність, яка приймає рішення про доступ на основі політики безпеки. Рішенням про доступ може бути «Дозволено», «Заборонено», «Не визначено» і множина зобов'язань (obligations), які повинен виконати PEP разом з виконанням рішення про доступ.

Ще одним атрибутом мови є політика (Policy) – множина правил (Rule), алгоритмів комбінування правил і політик і, можливо, множина зобов'язань. Політика може бути компонентом інших політик. У свою чергу, правило складається з мети, результату і умови і є компонентом політики. Кожен елемент правила може мати атрибути, які зберігаються в сховищі, званому Policy Information Point (PIP).

Відомо [3], що PEP виконує управління доступом, ґрунтуючись на відповідях, отриманих від PDP. PEP може бути реалізований у вигляді єдиного цілого з додатком, існувати як окремий об'єкт в тому ж контейнері, що й захищається додаток, або бути доступним у вигляді мережевого ресурсу.

Для опису процесу створення правил і політик вводиться поняття Точки адміністрування політики (Policy Administration Point – PAP) – системної сутності, за допомогою якої створюється одна або декілька політик.

Для перетворення запитів у вихідному форматі до формату XACML і конвертації рішення по авторизації в формат XACML до вихідного формату запиту вводиться поняття обробника запитів (Context handler).

Вдосконалена автором мова повинна включати в себе засоби завдання моделей розмежування доступу, які можуть мати післядії. При цьому розглядаються дії, які повинні бути виконані при кожній спробі доступу до ресурсів.

Слід зауважити, що також, як і у випадку з атрибутами безпеки, реалізація механізмів розмежування доступу на основі нової мови повинна підтримувати певний набір післядій. Для цього у вдосконаленій технології необхідно передбачити оброблювач післядій (Outcomes handler), який би дозволив після кожного застосування моделі до доступу виконувати післядії, що містяться в даній моделі.

Таким чином, потоки даних між системними сутностями, які беруть участь у прийнятті рішення, можуть бути представлені у вигляді моделі рис. 1.

Виходячи з основних правил і семантики побудови моделі, принципи управління доступом в комп'ютерній системі можна привести до такої послідовності:

– PAP створює політики, визначає алгоритми комбінування політик і робить їх доступними для PDP. Ці політики мають бути призначені для конкретних цілей і створені заздалегідь.

– Додаток надсилає запит на доступ до PEP.

– PEP надсилає запит на доступ до обробника запитів у форматі, який визначений у додатку, можливо додаючи атрибути суб'єктів, ресурсу, дії та оточення.

– Оброблювач запитів створює запит в форматі розробленого мови управління доступом і посилає його до PDP.

– PDP запрошувати будь-які додаткові атрибути суб'єкта, ресурсу, дії та оточення від оброблювача запитів.

– Оброблювач запитів перенаправляє запит атрибутів до PIP.

– PIP отримує запитані атрибути, можливо з різних джерел.

– PIP повертає запитані атрибути оброблювачу.

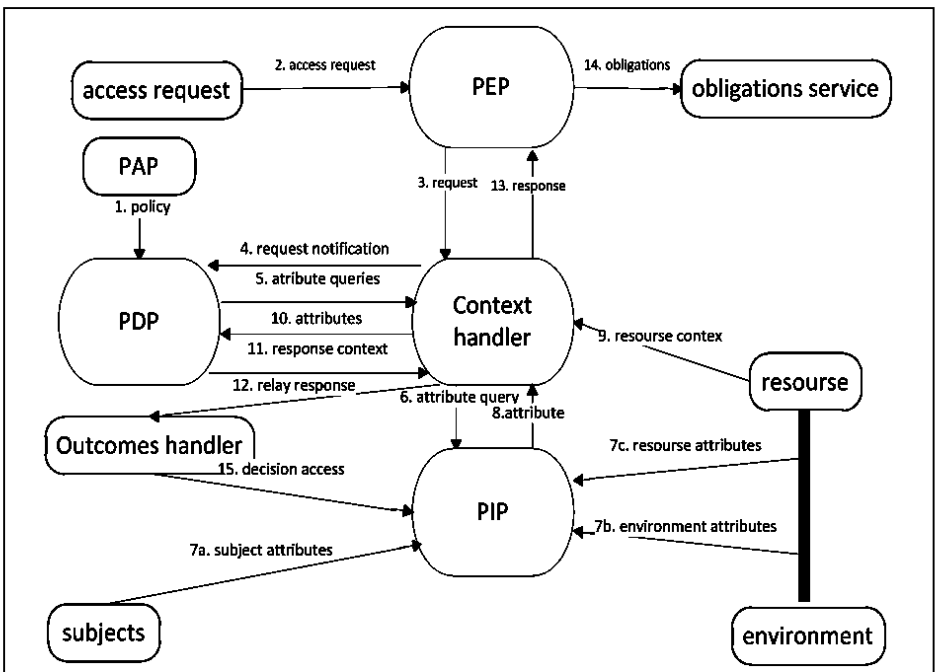

Рис. 1. Удосконалена модель потоків даних при розмежуванні доступу до комп'ютерної системи

– Оброблювач запитів може додати вміст ресурсу.

– Оброблювач запитів посилає запитані атрибути і, можливо, ресурс до PDP. PDP оцінює політику.

– PDP повертає відповідь, що містить рішення про можливість доступу оброблювачу запитів.

– Оброблювач запитів ретранслює рішення про можливість доступу на оброблювач післядій.

– Оброблювач запитів перетворює відповідь у вихідний формат, отриманий від PEP і повертає його PEP.

– PEP забезпечує управління доступом та виконання зобов'язань.

– Оброблювач післядії перетворює рішення про можливість доступу суб'єктів у встановлені атрибути, і посилає їх до PIP.

Рекомендації щодо практичного використання

Одним з практично значущих способів, що дозволяють оптимізувати вдосконалені механізми технології розмежування доступу, є спосіб, який називається еквівалентним перетворенням моделей. При цьому еквівалентним перетворенням називається перетворення однієї моделі розмежування доступу в іншу – таку, що всі доступи, які вирішуються першою, вирішуються і другою, при цьому виконуються необхідні післядії, і така ж умова є вірною для заборони доступів. Цей факт може бути використано для подальшого дослідження технології опису моделей розмежування доступу в комп'ютерній системі та вирішення оптимізаційних завдань моделювання.

Подальше дослідження передбачає розробку методик перевірки механізмів вдосконаленої технології розмежування доступу, проведення імітаційного моделювання та оцінку результатів проведених тестових випробувань.

Висновки

У статті запропонована вдосконалена технологія опису моделей розмежування доступу. Дана технологія відрізняється від відомих урахуванням фактора післядії в управлінні доступом до ресурсів комп'ютерних систем. Облік даного чинника в подальшому дозволить зменшити час на дозвіл запиту на доступ до комп'ютерної системи.

Список літератури

1. Андреев О.О. Интеграция моделей логического разграничения доступа, описанных на специализированном языке / О.О. Андреев // Информационные технологии. – М.: Новые технологии. – 2009. – № 12. – С. 29-33.

2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/printable_article?art_id=38934.

3. Лапонина О.Р. Анализ возможностей языка XACML по управлению доступом / О.Р. Лапонина // Сборник трудов V Международной научно-практической конференции "Современные информационные технологии и ИТ-образование" (8–10 ноября 2010 г.). – М: Московский госуд. университет им. М.В. Ломоносова. – С. 473-484.

4. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс]. – Режим доступу до ресурсу: http://tzi.com.ua/nd-tz-2.5-004-99.html.

5. Семенов С.Г. Методика настройки параметров распределения доступа и защиты информации в компьютерных системах критического применения / С.Г. Семенов // Системи озброєння і військова техніка. – Х.: ХУПС, 2012. – № 4(32). – С. 153-158.

6. Семенов С.Г. Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения / С.Г. Семенов. – Х.:НТУ «ХПИ», 2013. – 360 с.

Надійшла до редколегії 15.12.2014

Рецензент: д-р техн. наук, проф. О.О. Можаєв, Національний технічний університет «Харківський політехнічний інститут», Харків.

КОНЦЕПЦИЯ УСОВЕРШЕНСТВОВАННОЙ ТЕХНОЛОГИИ ОПИСАНИЯ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ ЗАЩИТЫ ДАННЫХ В КОМПЬЮТЕРНОЙ СИСТЕМЕ

С.Г. Семенов

Проведен анализ технологий описания моделей разграничения доступа к ресурсам компьютерных систем. Определенно, что одним из перспективных языков моделирование есть язык XACML. Определены основные его недостатки и предложена концепция, позволяющая учесть фактор последействия в процессе моделирования разграничения доступа к ресурсам. Усовершенствована модель потоков данных при разграничении доступа к компьютерной системе. Предложены рекомендации относительно практического использования. Сделан вывод о возможности уменьшения времени на разрешение запроса на доступ к компьютерной системе.

Ключевые слова: *защита данных, разграничения доступа, технологии описания моделей, язык XACML.*

CONCEPTION OF THE IMPROVED TECHNOLOGY OF DESCRIPTION OF MODELS OF DIFFERENTIATING OF ACCESS FOR DEFENCE OF INFORMATION IS IN COMPUTER SYSTEM

S.G. Semenov

The analysis of technologies of description of models of differentiating of access is conducted to the resources of the computer systems. Certainly, that one of perspective languages a design is language of XACML. His basic failings are certain and conception, allowing to take into account the factor of последействия in the process of design of differentiating of access to the resources, is offered. The model of flows of data is improved at differentiating of access to the computer system. Recommendations are offered in relation to the practical use. A conclusion is done about possibility of diminishing of time on permission of request for access to the computer system.

Keywords: *protection of data, differentiating of access, technologies of description of models, language of XACML.*