Розподілена авторизація в розподілених системах

Кирюша Б.А.
ННК ІПСА НТУУ «КПІ»

Поширення рішень побудованих на Інтернет-додатках та сервісів з використанням хмарних обчислень створює ситуацію, коли питання авторизації набувають принципово нових якостей. Авторизація окремого користувача викликає низку різних авторизацій на окремих ресурсах, які навіть не обов'язково мають єдину систему адміністрування безпеки. В даному випадку кожен адміністратор намагається щонайбільше захистити інтереси своєї мережі з власної точки зору. Централізувати систему керування безпекою в такій мережі принципово неможливо, оскільки сама система складається з незалежних сервісів за своєю суттю. Більше того, окремі політики безпеки також є розподіленими, залишаючи частини інформації про сесію як на серверах так і на комп'ютері користувача. В цій роботі проаналізовано можливості спрощення написання модулю авторизації для розподілених систем шляхом використання спеціалізованої мови $PCML_5$ [1].

Розподілена авторизація може бути представлена у вигляді послідовності конструкторів верхнього рівня абстракції. Такі конструктори поділяються на: властивості(значення, оператор prop), докази(процеси, оператор proof), твердження(виклики оператор affirmation). Головними перевагами такого набору операторів є чітке відображення послідовності дій, які має виконати система, при збереженні можливості автоматичної перевірки самого виразу, традиційним методом резолюції[2]

Вбудований в програму інтерпретатор $PCML_5$ забезпечує розробника можливістю уніфікувати процес викликів авторизації та обробки політик безпеки різних ресурсів з одного локального середовища. Сама мова не потребує дотримання жодних вимог окремих ресурсів. При цьому, зберігаються усі властивості політик авторизації. Наприклад, стає можливим з'ясовувати підчас тестування системи етапи, на яких розповсюдження інформації з авторизації користувача не відповідає власній політиці безпеки системи. Таким чином, стає можливим завчасно змінити використаний сервіс або подати запит на зміну політики безпеки сервісу по відношенню до створюваної системи.

Логічна перевірка виразів, яка є обов'язковою складовою роботи інтерпретатора $PCML_5$, не обмежується функцією синтаксичного аналізу. Лише за виконання вимоги логічної згортки виразу стає можливим автоматичний синтез послідовних звернень до систем авторизації з мінімальною кількістю таких викликів та забезпечується канонічна нормальна форма збереження всіх даних політик безпеки у внутрішній базі даних.

Нажаль, переваги обраного розробниками $PCML_5$ підходу до створення уніфікованої мови авторизації не виключають деяких суттєвих недоліків в практичній реалізації. Одним з них можна вважати відсутність текстового вводу програм. Замість цього до складу інтерпретатору додається програма графічного опису програми в позначенням, спеціально розроблених для $PCML_5$. Ці позначення є суто математичним, що ускладнює сприйняття результату програмістами, більш звичними до сучасних засобів програмування.

Складності з реалізацією програм мовою $PCML_5$ є одним з головних чинників, які стримують її широке вживання. Тому її розвиток буде цілком залежати від якості та простоти CASE засобів розробки програм в вихідному синтаксисі, або в спрощенні самого синтаксису до більш звичних сучасним програмістам форм.

Література

1. Kumar Avijit, Anupam Data, Robert Harper. Distributed programming with distributed authorization. Available at http://www.cs.cmu.edu/~kavijit/papers/pcml5-full.pdf
2. R. Harper, F. Honsell. A framework for defining logics.- Journal of the ACM, 1993.- p.143.