УДК 004.056

С.Г. Семенов, В.М. Зміївська, А.В. Голубенко

Національний технічний університет «Харківський політехнічний інститут», Харків

ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ РОЗМЕЖУВАННЯ ДОСТУПУ ДЛЯ ЗАХИСТУ ДАНИХ В КОМП'ЮТЕРНІЙ СИСТЕМІ

Проведено аналіз та порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерних системах. Розроблено класифікацію базових технологій розмежування доступу до ресурсів комп'ютерних систем. Виявлено низку характерних особливостей, переваг і недоліків існуючих напрямів і технологій управління доступом. Визначено, що одними з найбільш перспективних напрямів моделювання процесу розмежування доступу є суб'єктно-орієнтовані технології ізольованого програмного середовища.

Ключові слова: *захист даних, розмежування доступу, комп'ютерні системи, математичне моделювання.*

Вступ

Постановка задачі і аналіз літератури. Активне використання комп'ютерних систем для розв'язання широкого спектра практичних завдань вимагає підвищеної уваги розробників щодо питань інформаційної безпеки. Одним з аспектів цього питання є проблема розмежування доступу до інформаційних і функціональних ресурсів з метою забезпечення політик безпеки.

Аналіз літератури [1 – 6] та проведені дослідження показали, що в даний час існує безліч різних підходів, що визначають можливості учасників інформаційної взаємодії в доступі до тих або інших видів даних (ресурсів). При цьому основним з них є:

– технології систем дискреційного розмежування доступу;

– технології систем мандатного розмежування доступу;

– технології рольового розмежування доступу;

– суб'єктно-орієнтована технологія ізольованого програмного середовища.

Кожне з цих напрямків є описом набору правил, на підставі аналізу яких приймається рішення про доступ. Разом з тим, реалізація механізмів розмежування доступу до ресурсів кожної конкретної комп'ютерної системи, як правило, ґрунтується на більш складних, ніж базові технологіях, які враховують окремі особливості такої системи, середовища її оточення та положення політики її інформаційної безпеки. У кожному з цих випадків базові моделі або їх комбінації деталізуються цілим рядом додаткових обмежень і правил.

З метою вибору напрямку подальшого дослідження проведемо порівняльний аналіз базових технологій розмежування доступу до ресурсів комп'ютерних систем, що представлені на рис. 1.

Рис. 1. Класифікація базових технологій розмежування доступу до ресурсів комп'ютерних систем

Основна частина

Технології систем дискреційного розмежування доступу. Проведений аналіз технологій систем дискреційного розмежування доступу показал пріоритетність двох напрямів цього виду моделювання: матричного (модель Харрісона-Руззо-Ульмана (ХРУ), модель типізованих матриць доступу (ТМД)) і потокового (класична модель *Take–Grant*, розширена модель *Take-Grant*) [1, 4].

Основними елементами цих моделей є множина об'єктів системи $\{O\}$, множина суб'єктів системи $\{S\}$, множина видів прав доступу суб'єктів на об'єкти $\{R\}$, матриця доступів, рядки якої відповідають суб'єктам, а стовпці – об'єктам $M[s,o] \subseteq R$ (для моделей ХРУ і ТМД), кінцевий помічений орієнтований граф без петель, з множиною ребер $\{E\}$, що представляє поточні доступи до системи $G = (S, O, E)$ (для моделей *Take-Grant*). Вирішення задачі розмежування доступу в цих моделях зводиться до роз'вязання оптимізаційної задачі на матриці або графі [2].

Дискреційна технологія є однією з найбільш гнучких технологій розмежування доступу. Це є однією з головних причин її широкого розповсюдження. Але порівняльні дослідження цього напряму математичного моделювання дозволили виявити низку недоліків, що істотно знижують сферу застосування моделей.

Так, моделі ХРУ і ТМД можуть виражати велику різноманітність політик дискреційного розмежування доступу, але при цьому не надають алгоритмів перевірки їх безпеки. Також стає неможливим обмеження суб'єктів-власників об'єктів у наданні ними доступу іншим суб'єктам.

У той же час класична і розширена моделі *Take-Grant* при розширенні спектра політик безпеки стають занадто громіздкими, при цьому практичне їх використання значно ускладнюється.

Аналіз технологій мандатного розмежування доступу показав, що основу цього напряму становить моделювання засноване переважно на класичній моделі Белла – Ла Падула, описаній в 1975 році, яка призначена для аналізу систем захисту даних, що реалізовують мандатний розмежування доступу [5].

У класичній моделі Белла – Ла Падула аналізуються умови, при виконанні яких у комп'ютерній системі неможливе виникнення інформаційних потоків від об'єктів з великим рівнем конфіденційності до об'єктів з меншим рівнем зазначеної послуги безпеки.

Аналогічне узагальнення вказаного обмеження можна сформулювати й на інші послуги безпеки.

Основними елементами класичної моделі Белла–Ла Падула є: множина об'єктів системи $\{O\}$; множина суб'єктів системи $\{S\}$; множина видів доступу і видів прав доступу суб'єктів на об'єкти $\{R\}$; множина можливих поточних доступів до системи $B = \{b \subseteq S \times O \times R\}$; решітка рівнів конфіденційності $\{L\}$; матриця прав доступів $M[s,o] \subseteq R$, множина станів системи $\{V\}$; множина запитів системі $\{Q\}$; множина відповідей запитам $\{D\}$; функції, що визначають рівень доступу суб'єкта f_s; рівень конфіденційності об'єкта f_o; поточний рівень доступу суб'єкта f_{sc} та ін.

Безпека системи за допомогою даної моделі визначається на підставі трьох основних властивостей:

ss – властивості простої безпеки (*simple security*);

* – властивості зірка;

ds – властивості дискреційної безпеки (*discretionary security*).

При цьому розглядаються запити, що входять до множини $\{Q\}$:

– запити зміни множини поточних доступів b;

– запити зміни функцій f;

– запити зміни поточної структури дозволу доступу в матриці M.

Порівняльні дослідження моделі Белла – Ла Падула [1, 5] разом з її перевагами (можливість урахування широкого спектра запитів на розмежування доступу, висока міра надійності, чіткість формулювання правил та ін.) виявили й недоліки. Це, в першу чергу, складність практичної реалізації в повному об'ємі (перевірка безпеки системи вимагає перевірки нескінченної множини реалізацій системи), низька гнучкість системи моделювання для випадків виникнення нових видів доступу суб'єктів до об'єктів та ін.

Одним з продовжень напряму моделювання Белла – Ла Падула є модель Біба [6], що реалізовує мандатну політику цілісності. Аналіз цієї моделі показав, що основні її елементи не відрізняються від аналогічних елементів моделі Белла – Ла Падула, Крім того, так само як і в класичній моделі Белла – Ла Падула, в моделі Біба не розглядаються питання адміністрування рівнів цілісності суб'єктів і об'єктів. Проте, на відміну від моделі Белла-Ла Падула, вимоги безпеки в моделі Біба є динамічними; для їх опису використовуються елементи поточного і подальшого стану системи [1, 5, 6].

Незважаючи на це основні недоліки, що властиві моделі Белла – Ла Падула, мають місце і в моделі Біба.

Ще одним видом технології мандатного розмежування доступу став напрям систем військових повідомлень (СВП). Цей напрям орієнтований, у першу чергу, на системи прийому, передачі і обробки поштових повідомлень, що реалізовують мандатну політику безпеки.

У моделі СВП описуються чотири постулати безпеки, виконання яких потрібне для її коректної роботи [1].

1. Системний офіцер безпеки коректно дозволяє доступ користувачів до сутностей (об'єктів) і призначає рівні конфіденційності пристроїв і множини ролей.

2. Користувач призначає або перепризначає коректні рівні конфіденційності сутностей (об'єктів) при створенні або редагуванні в них інформації.

3. Користувач коректно направляє повідомлення по адресатах і визначає множину доступу до створених ним самим сутностей.

4. Користувач правильно визначає атрибут способу доступу до вмісту контейнера.

Аналіз моделі СВП показав, що, незважаючи на практичну реалізованість цього напряму формалізації, в ньому не міститься опису механізмів адміністрування. Зокрема, при описі функцій переходів пропущені такі можливі дії в системі, як створення нових сутностей, привласнення їм рівня конфіденційності і множини доступів.

Ще одним з основних напрямів опису процесу розмежування доступу в комп'ютерних системах є технології систем рольового розмежування доступу. Аналіз цих технологій показав, що рольове розмежування доступу є розвитком політики дискреційного розмежування доступу, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі.

Рольове розмежування доступу є складовою багатьох сучасних комп'ютерних систем. Як правило, рольове розмежування доступу застосовується в системах захисту СУБД або в елементах мережевих операційних систем.

В основі всіх математичних моделей цього напряму лежить базова модель рольового розмежування доступу, яка визначає найзагальніші принципи побудови ролей [1].

Основними елементами базової моделі рольового розмежування доступу є: множина користувачів $\{U\}$, множина ролей $\{R\}$, множина прав доступу на об'єкти комп'ютерної системи $\{P\}$, множина сесій користувача $\{S\}$, функція, що визначає для кожної ролі множину прав доступу $PA: R \to 2^P$, при цьому для кожного $p \in P$ існує $r \in R$ така, при якій $p \in PA(r)$, функція, що визначає для кожного користувача множину ролей, на які він може бути авторизований, а саме $UA: U \to 2^P$ та ін.

У базовій моделі рольового розмежування доступу існує низка обмежень, які дозволяють її використовувати в реальних комп'ютерних системах. Так, у базовій моделі рольового розмежування доступу відсутні механізми, що дозволяють одній сесії активізувати іншу (усі сесії активізуються користувачем). Ще одним важливим механізмом цього напряму моделювання є обмеження, що накладаються на множину ролей, на які може бути авторизований користувач або на які він авторизується в період однієї сесії [1].

Однією з відмітних особливостей цього напряму моделювання стала побудова системи адміністрування рольового розмежування доступу. Реалізація цього завдання покладена на відповідні моделі адміністрування, в яких адміністративні ролі можуть бути розділені на три групи за своїм призначенням (рис. 2):

– адміністрування множини авторизованих ролей користувачів;

– адміністрування множини прав доступу, які мають ролі;

– адміністрування ієрархії ролей.

Аналіз моделей адміністрування рольового розмежування доступу показав, що разом з безліччю переваг, основною з яких є простота їх практичного використання, існують недоліки, пов'язані з неможливістю врахування чинника зовнішніх впливів (у тому числі й зловмисних) на систему [1].

Аналогічні недоліки існують і в підході моделювання основаному на мандатно-рольовому розмежуванні доступу, орієнтованому на захист конфіденційності даних.

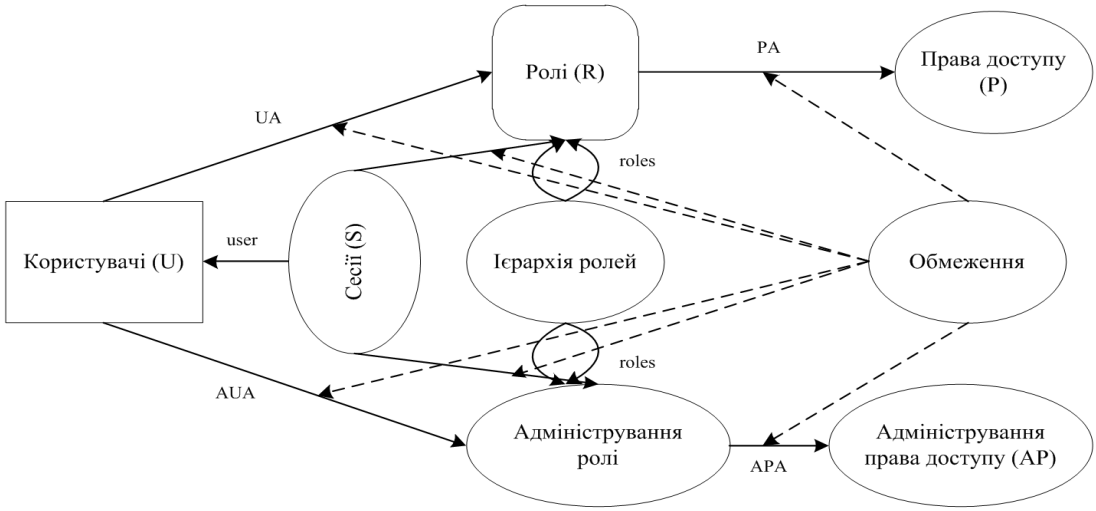
Як показали дослідження, врахування чинника суб'єктивного впливу на систему можливе шляхом використання суб'єктно-орієнтованих технологій, в яких основна увага приділяється визначенню порядку безпечної взаємодії суб'єктів системи, опису і обґрунтуванню необхідних умов реалізації в системі ізольованого програмного середовища [1 – 4].

У цих моделях основним суб'єктом, що реєструє зовнішні впливи на систему, є монітор звернень (індикативний або змістовний), а основним механізмом, який реалізовує політику безпеки в комп'ютеризованій інформаційній управляючій системі – монітор безпеки об'єктів.

Слід зауважити, що, хоча цей підхід моделювання враховує факт зовнішніх впливів на систему і його зручно використати для вирішення завдань виявлення і розпізнавання зовнішніх впливів, низка недоліків, пов'язаних з необхідністю уточнення окремих імовірнісно-часових характеристик і показників системи, вимагає додаткових досліджень і розробок.

Висновки

Проведені аналіз і порівняльні дослідження технологій розмежування доступу в комп'ютерних системах. У результаті проведених досліджень було виявлено низку характерних особливостей, переваг і недоліків існуючих напрямів управління доступом. Визначено, що одними з найбільш перспективних напрямів моделювання процесу розмежування доступу є суб'єктно-орієнтовані технології.



$APA : AR \to 2^{AP}$ – функція, що визначає для кожної адміністративної ролі множину адміністративних прав доступу, при цьому для кожного $p \in AP$ існує $r \in AR$ така, при якій $p \in APA(r)$;

$AUA : U \to 2^{AR}$ – функція, що визначає для кожного користувача множину адміністративних ролей, на які він може бути авторизований;

$roles : S \to 2^{R} \cup 2^{AR}$ – функція, що визначає для користувачів множину ролей, на які він авторизований у цій сесії, при цьому в кожен момент часу для кожного $s \in S$ виконується умова $roles(s) \subseteq UA\big(user(s) \cup AUA(user(s))\big)$.

Рис. 2. Структура основних елементів технології адміністрування рольового розмежування доступу

Список літератури

1. Девянин П.Н. Модели безопасности компьютерных систем / П.Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

2. 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.: ХУ ПС. – 2012. – Вип. 4(32). – С. 153-158.

3. 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.

4. Порошин С.М. Разработка и исследования математической модели компьютеризированной информационно-измерительной управляющей системы критического применения с учетом фактора внешних воздействий / С.М. Порошин, С.Г. Семенов // Системи обробки інформації. – Х.: ХУ ПС, 2013. – Вип. 2(110). – С. 208-210.

5. Bell D.E. Unified Exposition and Multics Interpretation MITRE Corporation / D.E. Bell, L.J. LaPadula // Secure Computer System: (1976). [Электрон. ресурс]. – Режим доступа к ресурсу: http://csrc.nist.gov/publications/history/bell76.pdf.

6. Biba K. Integrity Considerations for Secure Computer Systems / K. Biba // Technical Report MTR-3153, MITRE Corporation, Bedford, MA (Apr. 1977).

Надійшла до редколегії 18.12.2014

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

СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ ТЕХНОЛОГИЙ РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ ЗАЩИТЫ ДАННЫХ В КОМПЬЮТЕРНОЙ СИСТЕМЕ

С.Г. Семенов, В.М. Змиевская, А.В. Голубенко

Проведен анализ и сравнительные исследования технологий разграничения доступа для защиты данных в компьютерных системах. Разработана классификация базовых технологий разграничения доступа к ресурсам компьютерных систем. Обнаружен ряд характерных особенностей, преимуществ и недостатков существующих направлений и технологий управления доступом. Определенно, что одними из наиболее перспективных направлений моделирования процесса разграничения доступа есть субъектно-ориентированные технологии изолированной программной среды.

Ключевые слова: *защита данных, разграничения доступа, компьютерные системы, математическое моделирование.*

COMPARATIVE RESEARCHES OF TECHNOLOGIES OF DIFFERENTIATING ACCESS FOR INFORMATION DEFENCE IN COMPUTER SYSTEM

S.G. Semenov, V.M. Zmievska, A.V. Golubenko

An analysis and comparative researches of technologies of differentiating of access for defence of information is conducted in the computer systems. Classification of base technologies of differentiating of access is developed to the resources of the computer systems. Found out the row of characteristic features, advantages and lacks of existent directions and technologies of access control. Certainly, that one of the most perspective directions of design of process of differentiating of access are the subject-oriented technologies of the isolated software environment.

Keywords: *protection of data, differentiating of access, computer systems, mathematical design.*