Лабораторна робота №9.

Підсистема керування доступом

Мета роботи

ознайомити студентів з місцем та задачами підсистеми керування доступом в системах захисту інформації від несанкціонованого доступу.

Теоретичні відомості

Задачею підсистеми керування доступом в системах захисту інформації є виконання політики безпеки як певного набору правил розмежування доступу (ПРД).

Згідно матричної моделі безпеки, запропонованої Д. Деннінг, обчислювальну систему з точки зору безпеки можна описати у вигляді кортежу <S,O,A>, де S-множина суб'єктів системи, O-множина об'єктів системи, A-матриця доступу. Суб'єкти S є активними сутностями, здебільшого це користувачі або процеси. Об'єкти O є пасивними сутностями, тобто такими, що потребують захисту. Це можуть бути, наприклад, файли, записи баз даних, сегменти оперативної пам'яті. У деяких операціях доступу суб'єкти можуть виступати як пасивні сутності, до яких здійснюють доступ інші суб'єкти, тому $S \subset O$. У матриці доступу A кожен рядок відповідає певному суб'єктові S_i, а кожен стовпчик – об'єктові O_i. Елементом матриці $A(S_i, O_i)$ є список прав доступу, або повноважень суб'єкта S_i стосовно об'єкта O_i. Ці права, власне, і визначають, що може робити суб'єкт з об'єктом.

Оскільки матриця доступу, як правило дуже розріджена (і, отже, неефективна з точки зору використання пам'яті), вона практично не використовується в реальних системах у повному вигляді. Замість того використовуються її наявні представлення, а саме списки доступу та списки повноважень. Список доступу асоціюється з кожним захищеним об'єктом в системі і містить в собі ідентифікатори різних суб'єктів разом з їх правами доступу до даного об'єкту (список доступу, таким чином, відповідає стовпчику матриці доступу). На відміну від списку доступу, список повноважень асоціюється з кожним суб'єктом в системі і містить в собі ідентифікатори об'єктів разом з повноваженнями цього суб'єкта стосовно цих об'єктів. Список повноважень, таким чином, відповідає рядкові матриці доступу.

При використанні матричної моделі безпеки **політика безпеки інформації** набуває вигляду обмежень, що накладаються на спосіб модифікації матриці доступу. Так, у випадку **довірчого управління доступом** (згідно НД ТЗІ 1.1-003-99) всі права на зміну прав доступу до об'єкту надаються суб'єктові, що є власником цього об'єкту. Тобто, якщо список прав доступу суб'єкта S_i до об'єкта O_i містить право власника, то

суб'єкт S_i отримує повний контроль над стовпчиком матриці доступу, що відповідає O_i.

У випадку **адміністративного управління доступом** (НД ТЗІ 1.1-003-99) система захисту сама визначає можливість доступу суб'єктів до об'єктів, базуючись на певних мітках або атрибутах доступу, які може встановлювати або змінювати лише спеціально призначений адміністратор. Так, наприклад, в класичній **моделі Белла-ЛаПадула** такими атрибутами є рівень конфіденційності L та категорія C. При цьому мають виконуватись два правила: просте правило безпеки та *-правило. Просте правило безпеки встановлює, що суб'єкт S може читати об'єкт O тоді і тільки тоді, коли рівень конфіденційності $l_s \geq l_o$ та категорія $c_s \subseteq c_o$. *-правило встановлює, що суб'єкт S може писати в об'єкт O тоді і тільки тоді, коли рівень конфіденційності $l_s \leq l_o$ та категорія $c_o \subseteq c_s$.

Подальшим розвитком моделі Белла-ЛаПадула є **модель ватерлінії** (Low Water Mark, LWM). В цій моделі атрибути доступу об'єктів та суб'єктів можуть змінюватись у процесі роботи системи. Так, якщо суб'єкт S читає об'єкт O, рівень конфіденційності якого $l_s < l_o$, то рівень конфіденційності суб'єкта підвищується, так що $l_s = l_o$. І навпаки, якщо суб'єкт пише в об'єкт, коли $l_s > l_o$, то рівень конфіденційності об'єкта підвищується таким чином, що $l_s = l_o$.

Моделі Белла-ЛаПадула та ватерлінії сконцентровані на питаннях захисту обчислювальних систем від загрози конфіденційності інформації.

Інша група моделей безпеки (адміністративного управління доступом) розглядає питання захисту обчислювальних систем від загроз цілісності інформації. Так, в **моделі Біба** існують рівні цілісності **I** та категорії C. при цьому доступ суб'єкту до об'єкту на читання можливий тоді, коли $i_s \leq i_o$ та $c_s \subseteq c_o$. Доступ на запис, в свою чергу, можливий тоді і лише тоді, коли $i_s \geq i_o$ та $c_o \subseteq c_s$. Ці два правила, по аналогії з моделлю Белла-ЛаПадула, носять назву просте правило цілісності та *-правило цілісності. Існують також моделі Біба з пониженням рівня цілісності об'єкта та Біба з пониженням цілісності суб'єкта. В першій після операції запису суб'єктом S в об'єкт O рівень цілісності об'єкта падає до рівня цілісності суб'єкта ($i_s = i_o$). В другій внаслідок операції читання рівень цілісності падає до рівня цілісності прочитаного об'єкта ($i_s = i_o$).

Композитна модель адміністративного управління доступом об'єднує в собі модель конфіденційності Белла-ЛаПадула та модель цілісності Біба.

Хід роботи

1. Користуючись програмою, розробленою в ході Лабораторної роботи №7, розробіть програму, що давала б можливість працювати клієнту з об'єктами даних, що знаходиться на "серверному" боці. В якості об'єктів можуть виступати рядки символів або текстові файли. При цьому програма має реалізувати одну з політик контролю доступу згідно

наданому варіанту. Кількість прав доступу не повинна бути менше 4-х (враховуючи право власника).
2. Відлагодьте програму, користуючись інтерфейсом "зворотної петлі" (loopback), а потім – в спеціалізованій комп'ютерній лабораторії з реальними мережевими інтерфейсами.
3. Запротоколюйте роботу програми для не менш ніж трьох користувачів та не менш ніж десяти об'єктів даних.
4. Оформіть звіт.

Звіт має містити:

1) вихідні тексти клієнтської та серверної частин програми;
2) протокол роботи програми;
3) блок-схему; діаграму класів або модулів, або data-flow diagram (на вибір) та діаграму прецедентів розробленого ПЗ (виконуються за допомогою UML – ПЗ);
4) висновки.

Варіанти

Номер варіанту	**Політика контролю доступу**
1	Довірче (дискреційне) керування доступом
2	Модель Белла-ЛаПадула без категорій
3	Модель Белла-ЛаПадула з категоріями
4	Модель ватерлінії
5	Модель Біба без категорій
6	Модель Біба з категоріями
7	Модель Біба з пониженням рівню суб'єктів та об'єктів
8	Композитна модель

Контрольні запитання

1) Проаналізуйте недоліки довірчого управління доступом.
2) Оцініть позитивні та негативні сторони реалізованої політики безпеки.
3) Опишіть на рівні структур даних, як у Вашій роботі реалізовано матрицю доступу.
4) Охарактеризуйте рівень контролю доступу в реалізованій системі згідно НД ТЗІ 2.5-004-99. Що можна зробити, щоб його підвищити?
5) Проаналізуйте взаємодію підсистеми управління доступом автентифікації в розробленій системі