УДК 004.056

Н. Р. Кондратенко
Б. М. Свитка

МАТЕМАТИЧНА РЕШІТКА ЯК ОСНОВА РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ

Вінницький національний технічний університет

Анотація

Метою роботи є демонстрація ключової ролі теорії решіток як математичного фундаменту для побудови систем розмежування прав доступу. Розглянуто побудову решітки класів безпеки на основі аксіом Деннінга, та діаграми Гассе, та як за допомогою решіток будується чітка ієрархія рівнів доступу та категорій секретності. Також показано використання решіток на прикладі моделі Белла-ЛаПадула.

Ключові слова: решітка, діаграма Гассе, мандатне керування доступом, права доступу, захист інформації.

Abstract

The aim of the work is to demonstrate the key role of lattice theory as a mathematical foundation for building access rights delimitation systems. The construction of a lattice of security classes based on Denning's axioms and Hasse diagrams is considered, and how a clear hierarchy of access levels and categories of secrecy is built using lattices. The use of lattices is also shown using the example of the Bell-LaPadula model.

Keywords: lattice, Hasse diagram, mandated access control, access rights, information protection.

Вступ

Математична решітка — це впорядкована структура, яка визначає сувору ієрархію рівнів доступу та правила за якими інформація може переміщуватися між ними. Основний принцип решітки полягає в тому, що потік інформації дозволений лише в одному напрямку від нижчих рівнів до вищих, що повністю виключає можливість витоку конфіденційних даних на незахищені рівні.

Результати дослідження

Математично ця модель описується як впорядкована трійка $(SC, \leq, \oplus)$

SC – Множина класів безпеки

Це скінченна множина всіх міток доступу в системі. Кожному об`єкту і суб`єкту призначається одна така мітка з цієї множини.

$\leq$ – Відношення часткового порядку.

Для двох класів $A = (L_1, C_1)$ та $B = (L_2, C_2)$ дозволений потік інформації від A до B ($A \leq B$) тільки тоді коли:

1. $L_1 \leq L_2$ рівень безпеки B не нижчий за рівень A
2. $C_1 \subseteq C_2$ категорії A є підмножиною категорій B

Це відношення є рефлексивним, антисиметричним та транзитивним.

$\oplus$ – Об’єднання

Для будь-яких двох класів A та B результат $A \oplus B$ визначається як їхня найменша верхня межа.

$$(L_1, C_1) \oplus (L_2, C_2) = (max(L_1, L_2)\ C_1 \cup C_2)$$

Це гарантує, що новий об'єкт отримає найвищий із двох рівнів і всі категорії обох джерел одночасно.

Така структура базується на чотирьох аксіомах Деннінга.

1. Множина класів безпеки SC скінченна – це гарантує що система завжди зможе прорахувати допуск за рахунок скінченності множин.

2. Відношення на множині SC є відношенням часткового порядку. Це означає виконання трьох властивостей:

Рефлексивність – дані завжди можуть передаватися всередині одного класу.

Антисиметричність – якщо $A \leq B$ і з $B \leq A$, то $A = B$ – це однаковий рівень доступу.

Транзитивність – якщо $A \leq B$ та від $B \leq C$, то данні можуть передаватися від A до C.

3. У множині SC існує найменший елемент L_{min} такий що для будь-якого класу A виконується $L_{min} \leq A$.

4. Для будь-яких двох класів A та B $\in SC$ дія $\oplus$ завжди видає результат, який $\in SC$.

Виконання цих чотирьох аксіом означає, що структура $(SC, \leq, \oplus)$ утворює решітку, яку можна візуально зобразити на прикладі діаграми Гассе:

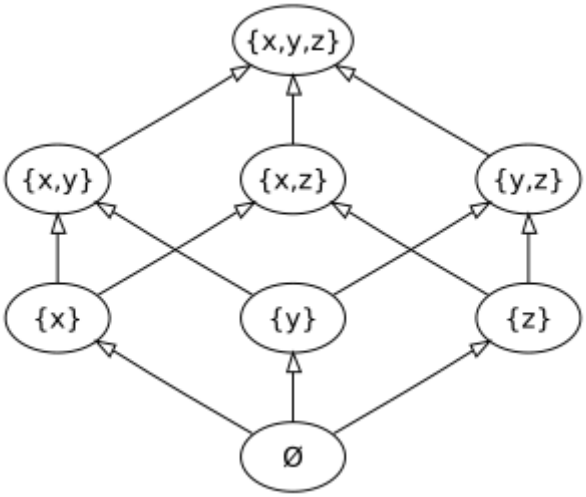

Рис. 1. Діаграма Гассе

Вузли діаграми представляють скінченну множину класів безпеки SC. Кожен вузол є унікальним кортежем видів доступу.

Ребра візуалізують відношення часткового порядку. Наявність ребра між двома вузлами вказує на пряме відношення домінування. Рух вгору по ієрархії відображає потік інформації від менш конфіденційного класу до класу з вищим рівнем допуску.

Найменший елемент ($\emptyset$) – це нижній вузол решітки, який відповідає мінімальному рівню безпеки з порожньою множиною категорій. Він не домінує над жодним іншим елементом, крім самого себе.

Найбільший елемент – це верхній вузол діаграми, який представляє найвищий рівень секретності та повний набір категорій (x, y, z). Цей елемент домінує над усіма іншими вузлами решітки, що надає йому повний доступ до всієї інформації в системі.

Саме ця решітка дозволяє практично використати її як фундамент для мандатної моделі розбежування доступа Белла-ЛаПадула. Ця модель грунтується на взаємодії між суб`єктами(користувачами) та об`єктами, в цій моделі використовуються такі права доступу як читання та запис інформації.

Основні компоненти цієї моделі:

S – множина суб’єктів

O – множина об’єктів

L – решітка рівнів безпеки.

A – множина прав доступу,{read, write}

$F: S \cup O \rightarrow L$ - функція класифікації, яка кожному суб'єкту та об'єкту присвоює певний рівень безпеки з решітки L.

Поточний стан системи описується як пара $v = (F, M)$ де M – матриця доступу елементи якої M[s,o] $\subseteq A$ визначають поточні права суб'єкта s щодо об'єкта o.

Безпека стану системи $v = (F, M)$ визначається через дві головні аксіоми:

1. Базова безпека(Simple Security):

Суб'єкт може отримати доступ на читання лише тоді, коли його вузол у решітці L розташований вище або на тому ж рівні, що й вузол об'єкта. Це забороняє рух інформації зверху вниз під час читання.

$$\forall_S \in S, \forall_O \in O : read \in M[s,o], then\ F(s) \geq F(o)$$

2. Зіркова властивість

Суб'єкт може здійснювати запис лише в об'єкти чий вузол у решітці L домінує над рівнем суб'єкта. Це гарантує, що інформація може рухатися по решітці лише знизу вгору, унеможливлюючи витік конфіденційних даних на нижчі рівні.

$$\forall_S \in S, \forall_O \in O : write \in M[s,o], \text{then } F(s) \leq F(o)$$

Стан v вважається повністю безпечним, якщо він задовольняє обидві аксіоми.

Висновки

Результати показало, що математичне обґрунтування доступу через решітки дозволяє побудувати надійну ієрархічну систему захисту. Використання часткового порядку для опису рівнів і категорій забезпечує чітку формалізацію правил безпеки. Наочне представлення структури у вигляді діаграм Гассе унеможливлює неоднозначність у правах доступу. Реалізація основних аксіом безпеки, зокрема моделі Белла-ЛаПадула, на базі решіток підтверджує можливість повного контролю за рухом секретної інформації. Це робить такий підхід ефективним інструментом для запобігання витокам даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sandhu R. S. Lattice-Based Access Control Models. Computer. 1993. Vol. 26, № 11. P. 9–19.
2. Bishop M. Computer Security: Art and Science. 2nd ed. Addison-Wesley Professional. 2018. 1440 p.
3. McLean J. Security Models. Naval Research Laboratory. 1994. 19 p.

Свитка Богдана Миколаївна — студентка групи 1ЕХКБ-25б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bogdanasvutka@gmail.com

Науковий керівник: ***Кондратенко Наталія Романівна*** — професор, Вінницький національний технічний університет, м. Вінниця, e-mail: kondratenko.natalia@vntu.edu.ua

Svitka Bohdana Mykolaivna — student of group 1EHKB-25b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bogdanasvutka@gmail.com

Scientific advisor: ***Kondratenko Nataliya Romanivna*** — professor, Vinnytsia National Technical University, Vinnytsia, e-mail: kondratenko.natalia@vntu.edu.ua