УДК 004.415.5
Било Н. – ст. гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ РОЗМЕЖУВАННЯ ДОСТУПУ МЕРЕЖОРІЄНТОВАНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ

Науковий керівник: к.т.н.,доц Осухівська Г.М.

Bylo N.
Ternopil Ivan Pul'uj National Technical

MATHEMATICAL AND SOFTWARE SYSTEMS CONCURRENT ACCESS NETWORK-BASED OPERATING SYSTEM

Supervisor: prof. Осухівська Г.М.

Ключові слова: методи доступу, розмежування прав.
Keywords: access methods ,permissions

З розвитком інформаційних технологій, покращилися і технології проникнення та несанкціонованого доступу до інформації, тому на сьогоднішній день при розробці систем захисту потрібно враховувати ряд умов, а саме: можливість виконання групами користувачів однакових обов'язків, можливість центрального адміністрування комп'ютерної системи, можливість передачі прав доступу користувачам разом із збереженням чіткого розмежування доступу, тощо. Потрібно також зазначити що одним із найефективніших методів захисту є модель рольової політики, вона прийшла на заміну дискреційній і мандатній. Це аргументується тим що вона як найкраще задовольняє всі вимоги цивільних комп'ютерних систем. Основою рольової політики є групи в UNIX системах, групування привілеїв в системах керування базами даних та концепція розмежування доступу. З математичної точки зору ієрархія – це частковий порядок, що визначає відношення старшинства між ролями. Старші ролі наслідують повноваження молодших, в той час як молодші – користувачів, асоційованих із старшими. Отже, модель ієрархії ролей визначає відношення включення між ролями, яке можна позначити " □□". R1 □□RR2 тільки якщо повноваження R2 є також повноваженнями R1, а користувачі R1 є також користувачами R2. Формально це можна виразити так:

$$R_1 \phi\ R_2 \Rightarrow \quad (authorized\_privileges(R_2) \subseteq authorized\_privileges(R_1)) \wedge$$
$$\wedge (authorized\_users(R_1) \subseteq authorized\_users(R_1)), R_1, R_2 \in \mathbf{R}$$
$$authorized\_users(R) = \{U \in \mathbf{U} \mid R' \phi\ R, (U, R') \in \mathbf{UA}\},\ R, R' \in \mathbf{R},$$
$$authorized\_privileges(R) = \{T \in \mathbf{T} \mid R' \phi\ R, (T, R') \in \mathbf{TA}\},\ R, R' \in \mathbf{R}.$$

Також дану модель можна визначити як багатозначне відношення між множинами користувачів і повноважень, що регламентується набором функціональних обов'язків фізичних користувачів. Не зважаючи на всі свої переваги, досі так і не створена універсальна модель яка б задовольняла усі критерії захисту комп'ютерних

систем. Зазвичай в мережорієнтованих ОС є три основних моделі доступу, це дискреційний, мандатний та на основі ролей.

Дискреційна модель управління доступу DAC. Доступ до системних ресурсів контролюється операційною системою (під контролем системного адміністратора), та дозволяє кожному користувачеві контролювати доступ до своїх даних. Прикладом реалізації даного доступу може бути ситуація коли одночасно в системі присутні як власники, які встановлюють права доступу до своїх об'єктів, так і суперкористувачі, що мають можливість зміни прав для будь-якого об'єкта та/або зміни його власника. Саме такий змішаний варіант реалізований в більшості операційних систем, наприклад Unix або Windows NT. Зокрема у Windows Server 2012 з'явилася нова концепція централізованого управління доступом до файлів і папок Dynamic Access Control. Основна відмінність нової системи від старої системи доступу до файлів і папок Access Control List (ACL - списки контролю доступу), полягає в тому, що за допомогою Dynamic Access Control (DAC) можна керувати доступом на основі практично будь-якого заданого атрибуту і навіть критерію.

Мандатний контроль доступу (MAC) є строгим на всіх рівнях управління і використовує ієрархічний підхід до управління доступом до ресурсів. Одним з видів реалізації мандатного управління доступом для UNIX систем став AppArmor. Його додали в SUSE Linux (в даний час підтримується Novell) і Ubuntu 7.10. AppArmor використовує функцію ядра Linux 2.6 - LSM (інтерфейс Linux Security Modules). LSM забезпечує API ядра, що дає можливість модулям ядра керувати контролем доступу. У Windows даний тип доступу реалізований примусовим контролем цілісності (MIC). Примусовий контроль цілісності (MIC) це функція ядра безпеки в Windows Vista і наступних поколінь систем Windows, яка додає *рівні цілісності* (IL) та ізолює робочі процеси. IL представляє рівень надійності об'єкта. Мета цього механізму полягає у використанні вже існуючої політики контролю цілісності та IL, вони беруть участь у процесі вибіркового обмеження права доступу в контекстах, які вважаються потенційно менш надійними, порівняно з іншими контекстами, що працюють під тим ж обліковим записом. Windows Vista визначає чотири рівні цілісності: Low (SID: S-1-16-4096), середній (SID: S-1-16-8192), високий (SID: S-1-16-12288), і система (SID : .. S-1-16-16384).

Управління доступом на основі ролей (Role Based Access Control, RBAC) – розвиток політики вибіркового керування доступом, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі. Використання RBAC для управління привілеями користувача (дозволу комп'ютера) в рамках єдиної системи або програми є широко поширена як найкращий варіант для управління. Зокрема, включаючи СКБД Oracle, PostgreSQL 8.1, SAP R/3, ISIS Papyrus, FusionForge, Wikipedia, Microsoft Lync, Microsoft Active Directory, Microsoft SQL Server і операційних системах, що використовують SELinux (Linux, Solaris і деякі інші Unix-подібні операційні системи), Grsecurity (Linux), TrustedBSD (FreeBSD). Також інші системи використовують різновиди підходу RBAC. Windows Server 2008, наприклад, підтримує функцію авторизації під назвою Windows Manager (AzMan), яка дає змогу створювати програми на основі RBAC.

Література:

1. Жора В. В. Підхід до моделювання рольової політики безпеки [Електронний ресурс] / В. В. Жора // Правове нормативне та метрологічне забезпечення систем захисту інформації в Україні : інтернет журн. – 2003. Вип. 7 [ст. 45 - 49] – Бібліогр.: 1 назва – Режим доступу: http://pnzzi.kpi.ua/7/07_p45.pdf

2. Windows Vista Integrity Mechanism Technical Reference [Електронний ресурс] Режим доступу: URL: https://msdn.microsoft.com/en-us/library/bb625964.aspx

3. SELinux Project Wiki [Електронний ресурс] Режим доступу: URL: http://selinuxproject.org/page/Main_Page