Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет безопасности информационных технологий

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

«Модели безопасности»

Выполнил:

студент группы N3246,

Суханкулиев Мухаммет

(подпись)

Проверила:

Коржук Виктория Михайловна

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

СОДЕРЖАНИЕ

Введение 3
1 Модель Белла и Лападула 4
1.1 Описание мандатного управления доступом 4
1.2 Основные идеи модели Белла и Лападулы 4
1.3 Формализация модели Белла и Лападулы 4
1.4 Расширение модели Белла и Лападулы на распределенные системы 6
1.5 Дополнительные аспекты модели 6
2 Пример 8
2.1 Контекст 8
2.2 Элементы системы модели Белла и Лападулы 8
2.3 Недостатки модели Белла и Лападулы 9
Заключение 10
Список использованных источников 11

ВВЕДЕНИЕ

Цель работы – изучить существующие модели безопасности и примеры их реализации.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Выбрать с преподавателем одну из рассмотренных на лекции моделей;
2. Тщательно изучить выбранную модель;
3. Придумать пример в реальной организации/информационной системе с использованием выбранной модели;
4. Составить презентацию с описанием и примером.

1 МОДЕЛЬ БЕЛЛА И ЛАПАДУЛА

1.1 Описание мандатного управления доступом

В отличие от дискреционного доступа (DAC), мандатный доступ (MAC) накладывает ограничения на передачу информации от одного пользователя другому. Это позволяет разрешить проблему троянских коней. Классической моделью, лежащей в основе построения многих систем MAC и породившей остальные модели MAC, является модель Белла и Лападула (БЛМ).

1.2 Основные идеи модели Белла и Лападулы

Идеи, лежащие в основе БЛМ, берут происхождение из "бумажного мира". Для предотвращения утечки информации к неуполномоченным субъектам этим субъектам с низкими уровнями безопасности не позволяется читать информацию из объектов с высокими уровнями безопасности. Это ведет к первому правилу БЛМ.

Простое свойство безопасности, также известное как правило **"нет чтения вверх" (NRU)**, гласит, что субъект с уровнем безопасности x_s может читать информацию из объекта с уровнем безопасности x_0, только если x_s преобладает над x_0.

Так же в правительстве США субъектам не позволяется размещать информацию или записывать ее в объекты, имеющие более низкий уровень безопасности. Например, когда совершенно секретный документ помещается в неклассифицированное мусорное ведро, может произойти утечка информации. Это ведет ко второму правилу БЛМ.

Свойство –*, известное как правило **"нет записи вниз" (NWD)**, гласит, что субъект безопасности x_s может писать информацию в объект с уровнем безопасности x_0 только если x_0 преобладает над x_s. Введение свойства –* разрешает проблему троянских коней, так как запись информации на более низкий уровень безопасности, типичная для троянских коней, запрещена.

Правило запрета по записи является большим упрощением некоторых реализаций БЛМ.

1.3 Формализация модели Белла и Лападулы

Обозначим:

S – множество субъектов;

O – множество объектов;

L – решётка уровней безопасности (уровни расположены в строгой иерархии);

$F: S \cup O \to L$ – функция уровня безопасности (определяет, какой уровень безопасности назначен объекту или субъекту);

V – множество состояний системы, где каждое состояние определяется F и M: матрицей доступа;

Матрица доступа M описывает, какие субъекты над какими объектами могут выполнять операции;

$$V = (F, M)$$

Процесс работы системы

Начальное состояние (v_0):

Система стартует с заданным состоянием: Все пользователи и объекты имеют назначенные уровни безопасности, а матрица доступа задана.

Запросы к системе (R):

R – это набор операций, которые субъекты хотят выполнить над объектами.

Функция переходов ($T: (V \times R) \to V$):

Описывает, как система меняет свое состояние V, обрабатывая запросы R. Система: Проверяет правила доступа ("NRU, NWD"). Если запрос разрешен, изменяет матрицу доступа M или состояние.

Определение 12.1. Состояние (F, M) безопасно по чтению (NRU) тогда и только тогда, когда для $\forall s \in S$ и для $\forall o \in O$, чтение $\in \mathrm{M}[s, o] \to F(s) \geq F(o)$.

Определение 12.2. Состояние (F, M) безопасно по записи (NWD, *- свойство) тогда и только тогда, когда для $\forall s \in S$ и для $\forall o \in O$, запись $\in \mathrm{M}[s, o] \to F(o) \geq F(s)$.

Определение 12.3. Состояние безопасно тогда и только тогда, когда оно безопасно по чтению и записи.

Основная теорема безопасности (ОТБ). Система (v_0, R, T) безопасна тогда и только тогда, когда состояние v_0 безопасно и T таково, что для любого состояния v, достижимого из V_0 после исполнения конечной последовательности запросов из $R, T(v, c) = v^*$, где $v = (F, M)$ и $v^* = (F^*, M^*)$, переходы системы (T) из состояния в состояние подчиняются следующим ограничениям для $\forall s \in S$ и для $\forall o \in \mathrm{O}$:

– если чтение $\in M^*[s, o]$ и чтение $\notin M[s, o]$, то $F^*(s) \geq F^*(o)$;

– если чтение $\in M[s, o]$ и $F^*(s) < F^*(o)$, то чтение $\notin M^*[s, o]$;

– если запись $\in M^*[s, o]$ и запись $\notin M[s, o]$, то $F^*(\mathrm{o}) \geq F^*(s)$;

– если запись $\in M[s, o]$ и $F(o) < F(s)$, то запись $\notin \mathrm{M}^*[s, o]$.

1.4 Расширение модели Белла и Лападулы на распределенные системы

Очевидным способом распространения БЛМ на распределенные системы будет назначение уровней безопасности различным компонентам и соблюдение гарантий выполнения правил-ограничений по чтению и записи.

В распределенной конфигурации чтение инициируется запросом от одного компонента к другому. Такой запрос образует прохождение потока информации в неверном направлении (запись в объект с меньшим уровнем безопасности). Таким образом, **удаленное чтение** в распределенных системах может произойти только если ему предшествует операция записи вниз, что является нарушением правил БЛМ. На практике достаточно внедрения в систему дополнительных средств обработки удаленных запросов для обеспечения того, чтобы поток информации от высокоуровневого субъекта к низкоуровневому объекту был ограничен запросом на доступ.

Так же можно сказать, что эти правила обеспечивают средства для предотвращения угрозы нарушения секретности для нормальных пользователей, но не говорят ничего по поводу той же проблемы для так называемых **доверенных субъектов**. Доверенные субъекты могут функционировать в интересах администратора. Также они могут быть процессами, обеспечивающими критические службы такие, как драйвер устройства или подсистема управления памятью. Такие процессы часто не могут выполнить свою задачу, не нарушая правил БЛМ. Одним из решений, рассматриваемых в литературе по безопасности, было предложение представлять и использовать для потока информации модель, требующую того, чтобы никакая высокоуровневая информация никогда не протекала на более низкий уровень. В данных моделях низкоуровневые пользователи не могут сделать выводы или затронуть работу высокоуровневых пользователей.

Если в некотором состоянии секретный субъект захотел прочитать совершенно секретный объект, то до тех пор, пока система удовлетворяет БЛМ, осуществить это будет невозможно. Но МакЛин заявляет, что ничто в БЛМ не предотвращает систему от **"деклассификации"** объекта от совершенно секретного до секретного (по желанию совершенно секретного пользователя).

1.5 Дополнительные аспекты модели

Все описанное выше является справедливым для модели БЛМ в "ее классической формулировке", кочующей из книги в книгу и из статьи в статью. Но в оригинальной

модели, представленной авторами, было введено требование сильного и слабого спокойствия. Данные требования снимают проблему Z–системы. Рассмотрим их.

Правило сильного спокойствия гласит, что уровни безопасности субъектов и объектов никогда не меняются в ходе системной операции.

Правило слабого спокойствия гласит, что уровни безопасности субъектов и объектов никогда не меняются в ходе системной операции таким образом, чтобы нарушить заданную политику безопасности.

Фактически **система Z** описывает алгебру моделей, самой строгой из которых (основание) является БЛМ с сильным спокойствием (ни один субъект модели не может изменить свою классификацию), а самой слабой (вершина) – БЛМ в классической формулировке, без ограничений для субъектов на изменение классификации.

Недостатком БЛМ, не рассмотренным нами ранее, является **отсутствие в модели поддержки многоуровневых объектов** (например, наличие несекретного параграфа в секретном файле данных) и отсутствие зависящих от приложения правил безопасности. С целью устранения данных недостатков при проектировании системы передачи военных сообщений (MMS) Лендвером и МакЛином была разработана модель MMS.

2 ПРИМЕР

2.1 Контекст

В МВД (Министерство внутренних дел) используется централизованная информационная система для работы с данными о гражданах, транспортных средствах, следственных делах и других конфиденциальных данных. Уровни доступа и субъектов в системе соответствуют строгой иерархии, чтобы предотвратить утечку информации.

2.2 Элементы системы модели Белла и Лападулы

Объекты:

1. Общедоступные сведения (статистические отчёты, информация о законодательных инициативах, объявления о работе в МВД);
2. Базы данных (личные данные граждан, включая адреса и паспортные данные);
3. Сведения о раскрытых преступлениях, информация о внутренних расследованиях МВД;
4. Сведения национальной безопасности (секретные оперативные мероприятия, информация о правительственных документах).

Объекты:

$$O = \{\text{Общедоступные сведения}, \text{Базы данных},$$
$$\text{Внутренние докуменеты МВД}, \text{Сведения национальной безопасности}\}$$

Субъекты:

$$S = \{\text{Гражджанин}, \text{Рядовой сотрудник},$$
$$\text{Следователь}, \text{Оперативный сотрадник}\}$$

Решётка уровней безопасности:

$$L = \{Unclassified, Confidential, Secret, Top\ Secret\}$$

Матрица доступа:

S\O	Общедоступные сведения	Базы данных	Внутренние документы МВД	Сведения национальной безопасности
Гражданин	чтение/запись	запись	запись	запись
Рядовой сотрудник	чтение	чтение/запись	запись	запись
Следователь	чтение	чтение	чтение/запись	запись
Оперативный сотрудник	чтение	чтение	чтение	чтение/запись

После каждого запроса R проверяется соответствие прав доступа согласно матрице. Запрос может быть отклонен или выполнен в зависимости от правил и уровней безопасности.

2.3 Недостатки модели Белла и Лападулы

1. Жёсткость правил доступа:

Модель затрудняет передачу данных между уровнями безопасности, требуя формальных процедур деклассификации, что может быть слишком медленным в критических ситуациях.

2. Отсутствие поддержки многоуровневых данных:

Документы с фрагментами разного уровня секретности требуют разделения или более гибких моделей, усложняя работу.

3. Уязвимость доверенных субъектов:

Доверенные субъекты (например, администраторы) могут быть скомпрометированы, что создаёт риск утечки данных, не предусмотренный моделью.

4. Сложность управления доступом:

Большое количество уровней безопасности делает управление доступом трудоёмким, увеличивая риск ошибок и замедляя работу системы.

ЗАКЛЮЧЕНИЕ

В ходе лабораторной работы я изучил основные принципы модели Белла и Лападулы. Полученные знания позволили понять, как мандатное управление доступом предотвращает утечку информации и обеспечивает защиту конфиденциальных данных. Кроме того, были выявлены преимущества и недостатки модели, что способствует её более глубокому пониманию и оценке применимости в различных системах безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ЛР 5 Модели безопасности - Google Документы
2. ТИБиМЗИ 5-6 лекция.pdf - Google Диск
3. Теоретические основы компьютерной безопасности, часть 2: Зарождение компьютерной безопасности / Хабр
4. Bell–LaPadula model - Wikipedia