УДК 681.3

МОДЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КРИТИЧНЫХ ИНФОРМАЦИОННО - ИЗМЕРИТЕЛЬНЫХ СИСТЕМ

(Часть 3.Модели мандатного доступа)

Артамонов В.А.

Белорусский национальный технический университет, Минск, Республика Беларусь

Рассмотрен класс моделей информационных технологий критичных ИИС на основе предоставления прав в виде мандатного доступа к объектам комплексных измерений. Представлены основные теоремы безопасности систем подобного класса.

Введение

Описанные в части 2 модели дискреционного доступа хотя и обеспечивают гранулированную защиту, но обладают рядом недостатков. В частности, в системах, построенных на основе ***DAC***, существует проблема троянских *программ (троянских коней)*. Троянскую программу следует определять как любую программу, от которой ожидается выполнение некоторого желаемого действия, а она на самом деле выполняет какое-либо неожиданное и нежелательное действие. Так, троянская программа может выглядеть как вполне хороший продукт, но реально она может оказаться даже более опасной, чем можно было бы ожидать. Для того чтобы понять, как может работать *троянский конь*, вспомним, что когда пользователь вызывает какую-либо программу на компьютере, в системе инициируется некоторая последовательность операций, зачастую скрытых от пользователя. Эти операции обычно управляются операционной системой. Троянские программы рассчитывают на то, что когда пользователь инициирует такую последовательность, он обычно верит в то, что система произведет ее, как полагается. При этом нарушитель может написать версию троянской программы, которая будучи запущенной от имени пользователя-жертвы, передаст его информацию пользователю нарушителю. В отличие от ***DAC***, мандатный доступ - ***MAC*** накладывает ограничения на передачу информации от одного пользователя другому. Это позволяет разрешить проблему троянских коней.

Основная часть

Классической моделью, лежащей в основе построения многих систем ***MAC*** и

породившей остальные модели, является модель Белла и Лападула (БЛМ) [1].

Идеи, лежащие в основе БЛМ, берут происхождение из "бумажного мира" путём перенесения модели безопасности, принятой при работе с документами, в мир компьютерных систем. Основным свойством, определяющем аналогичность требований безопасности, является то, что все субъекты и объекты ассоциируются с уровнями безопасности, варьирующимися от низких уровней (неклассифицированных) до высоких (совершенно секретных). Кроме того, для предотвращения утечки информации к неуполномоченным субъектам не позволяется читать информацию из объектов с высокими уровнями безопасности. Это является первым правилом БЛМ, известным как *« простое свойство безопасности»[1].*

Простое свойство безопасности, также известное как правило "нет чтения вверх" ***(NRU),*** гласит, что субъект с уровнем безопасности $\mathbf{x_s}$ (понятие уровня безопасности введено в части1) может читать информацию из объекта с уровнем безопасности $\mathbf{x_o}$, только если $\mathbf{x_s}$ преобладает над $\mathbf{x_o}$. Это означает, что если в системе, удовлетворяющей правилам модели БЛМ, субъект с уровнем доступа ***секретный*** попытается прочитать информацию из объекта, классифицированного как ***совершенно секретный***, то такой доступ не будет разрешен.

Дополнительное наблюдение в части секретного документооборота выявило неукоснительное требование: 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 – ***Свойству-*.***

Свойство-,* известное как правило "нет записи вниз" ***(NWD),*** гласит, что субъект безопасности $\mathbf{x_s}$ может писать информацию в объект с уровнем безопасности $\mathbf{x_o}$ только если $\mathbf{x_o}$ преобладает над $\mathbf{x_s}$. Это означает, что если в системе, удовлетворяющей правилам модели БЛМ, субъект с уровнем доступа совершенно секретный попытается записать информацию в неклассифицированный объект, то такой доступ не будет разрешен. 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. Так, некоторые описания включают более детальное понятие типа доступа (например такие, как добавление и выполнение). Помимо этого многие модели БЛМ включают понятие дискретной защиты с целью обеспечения хорошо гранулированной защиты при сохранении всех преимуществ БЛМ.

Правила запрета по записи и чтению БЛМ отвечают интуитивным понятиям того, как предотвратить утечку информации к неуполномоченным источникам.

Рассмотрим формализацию БЛМ. В соответствии с определениями части 1:

S - множество субъектов;

O - множество объектов;

L - решетка уровней безопасности;

F : S∪O →*L* - функция, применяемая к субъектам и объектам; данная функция определяет уровни безопасности своих аргументов в данном состоянии;

V - множество состояний - множество упорядоченных пар **(F, M),** где **M** - матрица доступа субъектов системы к объектам.

Система представляется начальным состоянием $\mathbf{v_0}$, определенным множеством запросов к системе **R** и функцией переходов **T : (V×R) → V** такой, что система переходит из состояния в состояние после исполнения запроса. Сформулируем определения, необходимые для доказательства основной теоремы безопасности (ОТБ).

*Определение 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* $\in M[s, o] \rightarrow F(s) \geq F(o)$.

*Определение 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* $\in M[s, o] \rightarrow F(o) \geq F(s)$.

Определение 3. Состояние безопасно тогда и только тогда, когда оно безопасно по чтению и записи.

Теорема (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* $\forall o \in O$*:*

- 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* $\in M^* [s, o]$ *;*

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

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

Доказательство[2].

1. *Необходимость.* Предположим, система безопасна. Состояние $\mathbf{v_0}$ без опасно по определению. Если имеется некоторое состояние ***v***, достижимое из состояния $\mathbf{v_0}$ после исполнения конечной последовательности запросов из **R** таких, что **T(v, c) = v*** , хотя **v*** не удовлетворяет одному из двух первых

ограничений для **T**, то **v*** будет достижимым состоянием, но противоречащим ограничению безопасности по чтению. Если **v*** не удовлетворяет одному из двух последних ограничений для **T**, то **v*** будет достижимым состоянием, но противоречащим ограничению безопасности по записи. В любом случае система небезопасна.

2. *Достаточность*. Предположим, что система небезопасна. В этом случае либо $\mathbf{v_0}$ должно быть небезопасно, либо должно быть небезопасно состояние **v**, достижимое из состояния $\mathbf{v_0}$ после исполнения конечной последовательности запросов из **R**. Если $\mathbf{v_0}$ небезопасно - все доказано. Если $\mathbf{v_0}$ безопасно, допустим, что **v***- первое в последовательности запросов небезопасное состояние. Это означает, что имеется безопасное состояние **v** такое, что **T(v,c) = v*** , где **v*** - небезопасно. Но это противоречит четырем ограничениям безопасности на **T**.

Несмотря на все достоинства, оказалось, что при использовании БЛМ в контексте практического проектирования и разработки реальных систем информационных технологий возникает ряд технических вопросов, которые являются логическим следствием достоинства БЛМ - ее простоты. Проблемы возникают при рассмотрении вопросов построения политик безопасности для конкретных типов систем, то есть на менее абстрактном уровне рассмотрения. При данном рассмотрении системный компонент модели усложняется, что может привести к неадекватности БЛМ в ее классической форме. Как следствие, в мире компьютерной безопасности ведется широкая полемика по поводу применимости БЛМ для построения безопасных систем.

Рассмотрим ряд примеров *критики* БЛМ. Некоторые из них взяты из литературы, посвященной вопросам безопасности, другие часто включаются в описание политик безопасности и представляют собой так называемую «обязательную критику» БЛМ.

Начнем данное рассмотрение с обсуждения проблемы, возникающей в распределенных системах, удовлетворяющих правилам БЛМ. В частности, покажем, что запрос на *чтение* вызывает «протекание» потоков информации в обоих направлениях между компонентами, что является нарушением правил модели. Затем рассмотрим проблему использования этой модели для обеспечения безопасности доверенных субъектов, которые выполняют наиболее критичные задачи в системе ИТ. Завершим обсуждение примером описания модели, известной как ***система Z*** [3].

Удаленное чтение

В свете тенденций использования распределенных конфигураций ИИС требуется

рассматривать модели безопасности не только для автономных, но и для распределенных систем ИТ (распределенная система обычно состоит из нескольких объединенных систем). Очевидным способом распространения БЛМ на распределенные системы будет назначение уровней безопасности различным компонентам и соблюдение гарантий выполнения правил-ограничений по чтению и записи.

Например, некоторым компонентам можно назначить уровни безопасности, меняющиеся от неклассифицированного до совершенно секретного уровня, и на основании принципов БЛМ синтезировать соединения между различными компонентами системы. Может показаться, что если конфиденциальному субъекту **A** будет разрешено чтение информации из неклассифицированного объекта **B**, никакая конфиденциальная информация не будет раскрыта. Но при более подробном рассмотрении реализации операции удаленного чтения снизу может быть сделано неприятное наблюдение. Операция чтения между удаленными компонентами приводит к протеканию потока информации от читаемого объекта к запросившему доступ на чтение субъекту. Данный поток является безопасным, поскольку информация не разглашается неавторизованному субъекту. Однако 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. Многие исследователи рассматривают эту проблему как наиболее убедительное свидетельство неадекватности БЛМ. Однако на практике эта проблема часто является несущественной; 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. Фактически, некоторые архитектуры предлагают отдельные компоненты, выполняющие обработку таких запросов и потока информации в распределенных системах.

Доверенные субъекты

В предыдущем описании правил БЛМ не было указано, какие субъекты должны подчиняться этим правилам. Например, компьютерные системы обычно имеют администратора, который управляет системой, добавляя и удаляя пользователей, восстанавливает функционирование после сбоев, устанавливает специальное программное обеспечение, устраняет ошибки в операционной системе или

приложениях и т.п. Очевидно, что процессы, действующие в интересах таких администраторов, не могут управляться правилами БЛМ или каких-либо других моделей, не позволяющих им выполнять функции администрирования.

Это наблюдение высвечивает еще одну техническую проблему, связанную с правилами БЛМ. 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. Неприменимость БЛМ для доверенных субъектов может быть выражена путем внесения поправки в данное ранее определение операций чтения и записи БЛМ. Но хотя это и делает определение более точным, оно нисколько не облегчает задачу для разработчика, желающего построить безопасный драйвер или утилиту поддержки работы администратора.

Одним из решений, рассматриваемых в литературе по безопасности, было предложение представлять и использовать для потока информации модель, требующую реализации политики безопасности такой, чтобы никакая высокоуровневая информация никогда не протекала бы на более низкий уровень.

Система Z как попытка решения проблемы БЛМ

В работе [3] представлено концептуальное описание системы, названной ***система Z***. Из чего следует, что любая система, удовлетворяющая правилам БЛМ, может иметь ряд проблем с секретностью. При этом, сама ***Система Z*** выражается в терминах набора субъектов и объектов, с каждым из которых связан уровень безопасности. Совокупность уровней безопасности для каждого субъекта и объекта в некоторый момент времени описывает состояние системы. ***Система Z*** удовлетворяет БЛМ, если во всех состояниях системы комбинации уровней субъектов и объектов таковы, что в этом состоянии никакой субъект не может осуществить запись вниз или чтение сверху.

Предположив, что ***система Z*** удовлетворяет условиям БЛМ, можно быть уверенным, что любая угроза секретности будет обнаружена. Однако существует одна техническая деталь, которая не очевидна в таких системах. Если в некотором состоянии *секретный* субъект захотел прочитать *совершенно секретный* объект, то до тех пор, пока система удовлетворяет БЛМ, осуществить это будет невозможно. Однако, ничто в БЛМ не

предотвращает систему от "деклассификации" объекта от *совершенно секретного* до *секретного* (по желанию *совершенно секретного* пользователя).

В качестве иллюстрации можно привести следующий пример. Допустим, субъект с высокой степенью доверия **A** читает информацию из объекта, уровень классификации которого также равен **A**. Далее данный субъект понижает свою степень доверия до уровня **B (A > B)**. После этого он может записать информацию в файл с классификацией **B**. Нарушения БЛМ формально не произошло, но безопасность системы нарушена.

Фактически ***система Z*** описывает конфигурацию, в которой все субъекты могут читать и записывать любой объект путем назначения соответствующих уровней безопасности объекта перед выполнением запросов на доступ. В такой системе, которая очевидно не обеспечивает секретность информации, все состояния могут быть рассмотрены как удовлетворяющие требованиям БЛМ.

Все описанное выше является справедливым для модели БЛМ в "ее классической формулировке". Но в оригинальной модели [1, 2] было введено требование *сильного* и *слабого* спокойствия. Данные требования снимают проблему ***Z-системы***.

Правило *сильного спокойствия* гласит, что уровни безопасности субъектов и объектов никогда не меняются в ходе системной операции. Реализовав это правило в конкретной системе, можно легко сделать заключение, что описанный выше тип потенциальных проблем никогда не произойдет. Очевидным недостатком такой реализации в системе является потеря гибкости при выполнении операций.

Правило *слабого спокойствия* гласит, что уровни безопасности субъектов и объектов никогда не меняются в ходе системной операции таким образом, чтобы нарушить заданную политику безопасности. Это правило может потребовать, чтобы субъекты и объекты воздерживались от действий в период времени, когда меняются их уровни безопасности. Например, может потребоваться, чтобы уровень безопасности объекта никогда не менялся в то время, как к нему обращается некоторый субъект. Однако, если операция чередуется с изменением уровня безопасности, не вызывающего нарушения безопасности (например, субъект повышает свой уровень с *секретного* до *совершенно секретного* в ходе выполнения операции чтения неклассифицированного объекта), то правило слабого спокойствия будет по прежнему соблюдено.

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.

Заключение

Как было отмечено в настоящей части, одним из недостатков, являющимся логическим следствием достоинства простоты БЛМ, является ее слишком большая абстрактность. С точки зрения требований пользователей, в реальных приложениях ограничения, накладываемые БЛМ, оказываются слишком строгими. Введение в модель доверенных процессов, позволяющих частично решить данную проблему, не является достаточным. С другой стороны, 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 ИТ критичных ИИС следует адаптировать БЛМ для условий и предположений безопасности для информационных технологий ИИС чувствительных к передаче измерительного и управляющего трафика, в том числе и для военных (ядерных) сообщений – **MMS** [4].

Список цитируемых источников

1. Bell L. LaPadula. Secure Computer System: Mathematical Foundation, ESD-TR-73-278, V 1, MITRE Corportation.

2.LaPadula D. Bell. Secure Computer Systems: A Mathematical Model, ESD-TR-73-278, V. II, MITRE Corportaion.

3. John McLean "A comment on the "Basic Security Teorem" of Bell and La Padula", Information Processing Letters, 1985.

4. Carl E. Lendwehr, Constanse L.Heitmeyer, John McLean, "A security models for military message system", ACM transactions of computer systems, 1984.

Artamonov V.A.

The models of safety information technologies critical information-measuring systems (Part 3. The models of mandatory access)

The class of models of information technologies critical IMS on the basis of granting the rights in the form of mandatory access to objects of complex measurements is considered.The basic theorems of safety's systems of a similar class are presented.