УДК 681.3

МОДЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КРИТИЧНЫХ ИНФОРМАЦИОННО - ИЗМЕРИТЕЛЬНЫХ СИСТЕМ

(Часть 4. Модификация модели мандатного доступа для военных и ядерных систем)

Артамонов В.А.

Белорусский национальный технический университет, Минск, Республика Беларусь

Рассмотрена модель информационных технологий критичных ИИС на основе предоставления прав в виде мандатного доступа к объектам комплексных измерений, модифицированная для военных и ядерных приложений. Представлены основные предположения и ограничения для данного вида модификаций. Предложена неформализованная модель описания процессов предоставления прав для систем подобного класса.

Введение

Как нами уже было отмечено в предыдущей части, платой за простоту мандатной модели БЛМ является её абстрактность. Как следствие этого обстоятельства при разработке политик безопасности для отдельных категорий критичных объектов требуется введение отдельных ограничений и предположений безопасности информационных технологий (ИТ) при реализации информационно-измерительных систем (ИИС) для обслуживания управляющего и измерительного трафика. Ярким примером специализации модели БЛМ является её модификация для военных и ядерных приложений – *Security models for military message system (MMS)* [1].

Специализированная модель MMS

В модели MMS используются следующие определения.

Классификация - обозначение, накладываемое на информацию, отражающее ущерб, который может быть причинен неавторизованным доступом; включающее уровни: ***TOP SECRET***, ***SECRET*** и т.д. и множество меток (***"CRYPTO", "NUCLEAR"*** и т.д.). Множество классификаций и отношение между ними образуют решетку.

Степень доверия пользователю - уровень благонадежности персоны. Каждый пользователь имеет степень доверия, и операции, производимые системой для данного пользователя, могут проверить степень доверия пользователю и классификацию объектов, с которыми он оперирует.

Пользовательский идентификатор - строка символов, используемая для того, чтобы отметить пользователя системы. Для использования системы пользователь должен предъявить ей пользовательский идентификатор, и система должна провести аутентификацию пользователя. Данная процедура называется login. Каждый пользователь должен иметь уникальный идентификатор.

Пользователь - персона, уполномоченная для использования системы.

Роль - работа, исполняемая пользователем (например пользователь, имеющий право удалять, распространять или понижать классификацию объектов). Пользователь всегда ассоциирован как минимум с одной ролью в некоторый момент времени, и он может менять роль в течение сессии. Для действий в данной роли пользователь должен быть уполномочен. Некоторые роли могут быть связаны только с одним пользователем в данный момент времени. С любой ролью связана способность выполнения определенных операций.

Объект - одноуровневый блок информации. Это минимальный блок информации в системе, который имеет классификацию. Объект не содержит других объектов, он не многоуровневый.

Контейнер - многоуровневая информационная структура. Имеет классификацию и может содержать объекты (каждый со своей классификацией) и (или) другие контейнеры. Файл - это *контейнер*. Некоторые структуры файла могут быть *контейнерами*. Различие между *объектом* и *контейнером* базируется на типе, а не на текущем содержимом: если один из файлов данного типа является контейнером, то все остальные файлы данного типа являются контейнерами, даже если некоторые из них содержат только объекты или пусты. Устройства такие, как диски, принтеры, ленты, сетевые интерфейсы и пользовательские терминалы - контейнеры.

Сущность – любая именованная (т.е. имеющая имя) составляющая системы ИТ, например о*бъект* или *контейнер* (файл, диск и т.д.).

Требование степени доверия контейнеров - атрибут некоторых *контейнеров*. Для некоторых *контейнеров* важно требовать минимум степени доверия, то есть пользователь, не имеющий соответствующего уровня благонадежности, не может просматривать содержимое *контейнера*. Такие *контейнеры* помечаются соответствующим атрибутом **(CCR).** Например, пользователь, имеющий степень доверия ***CONFIDENTAL***, не может просматривать ***CONFIDENTAL*** параграф сообщения, помеченного ***TOP SECRET***, если оно содержится в **CCR** *контейнере*. Если пользователь должен иметь возможность просматривать данное сообщение, *контейнер* не должен быть помечен как **CCR**.

Идентификатор (ID) - имя сущности без ссылки на другие сущности, например, имя файла есть идентификатор этого файла. Обычно все сущности имеют идентификатор.

Ссылка на сущность *прямая,* если это идентификатор *сущности*.

Ссылка на сущность *косвенная,* если это последовательность двух или более имен *сущностей* (из которых только первая - *идентификатор*). Пример: "текущее сообщение, первый абзац, вторая строка".

Операция - функция, которая может быть применена к сущности. Она может позволять просматривать или модифицировать сущность. Некоторые операции могут использовать более одной сущности (пример - операция копирования).

Множество Доступа - множество троек *(Пользовательский идентификатор или роль, Операция, Индекс операнда)*, которые связаны с *сущностью*. Операция, которая может быть специфицирована для особых сущностей, зависит от типа данной сущности. Если операция требует более одного операнда, индекс операнда специфицирует позицию, на которой ссылка на данный операнд может появиться в операции.

Сообщение - особый тип, реализуемый в MMS. *Сообщение* является *контейнером*. *Сообщение* включает поля *куда, откуда, время, предмет, текст, автор*. Чертежные сообщения включают поле чертежа.

Неформальная модель MMS

Пользователь получает доступ к системе только после прохождения процедуры ***login***. Для этого пользователь предоставляет системе *Пользовательский идентификатор,* и система производит аутентификацию, используя пароли, отпечатки пальцев или другую адекватную технику. После успешного прохождения аутентификации *Пользователь* запрашивает у системы *Операции* для использования функций системы. *Операции,* которые *Пользователь* может запросить у системы, зависят от его *ID* или *Роли,* для которой он авторизован: с использованием *Операций* пользователь может просматривать или модифицировать *Объекты* или *Контейнеры*. Система реализует ограничения, описанные ниже.

Предположения Безопасности

Пользователь всегда может скомпрометировать информацию, к которой он имеет законный доступ. Таким образом, надо сформулировать предположения безопасности, которые могут быть выполнены только пользователями системы.

A1. Администратор/офицер безопасности системы присваивает уровни доверия, классификацию устройств и множества ролей корректно.

A2. Пользователь вводит корректную классификацию, когда изменяет, объединяет или переклассифицирует информацию.

A3. Пользователь классифицирует сообщения и определяет множества доступа для сущностей, которые он создает, так, что только пользователь с требуемой благонадежностью может просматривать информацию.

A4. Пользователь должным образом контролирует информацию объектов, требующих благонадежности.

Ограничения безопасности

Ограничения безопасности, в отличие от предположений безопасности, должны поддерживаться не пользователями системы, а непосредственно ИТ-системой.

B1. Авторизация – пользователь может запрашивать операции над сущностями, только если пользовательский идентификатор или текущая роль присутствуют во множестве доступа сущности вместе с этой операцией и со значением индекса, соответствующим позиции операнда, в которой сущность относят в требуемой операции.

B2. Классификационная иерархия – классификация контейнера всегда больше или равна классификации сущностей, которые он содержит.

B3. Изменения в объектах – информация, переносимая из объекта, всегда наследует классификацию данного объекта. Информация, вставляемая в объект, должна иметь классификацию ниже классификации этого объекта.

B4. Просмотр – пользователь может просматривать (на некотором устройстве вывода) только сущности с классификацией меньше, чем классификация устройства вывода и степень доверия к пользователю (данное ограничение применяется к *сущностям, адресуемым прямо или косвенно).*

B5 Доступ к контейнерам, требующим степени доверия – пользователь может получить доступ к косвенно адресованной сущности внутри контейнера, требующего степени доверия, только если его степень доверия не ниже классификации контейнера.

B6. Преобразование косвенных ссылок – пользовательский идентификатор признается законным для сущности, к которой он обратился косвенно, только если он авторизован для просмотра этой сущности через ссылку.

B7. Требование меток - сущности, просмотренные пользователем, должны быть помечены его степенью доверия..

B8. Установка степеней доверия, ролей, классификации устройств – только пользователь с ролью офицера безопасности системы может

устанавливать данные значения. Текущее множество ролей пользователя может быть изменено только офицером безопасности системы или самим пользователем.

B9. Понижение классификации информации – никакая классифицированная информация не может быть понижена в уровне своей классификации, за исключением случая, когда эту операцию выполняет пользователь с ролью *"пользователь, уменьшающий классификацию информации".*

B10. Уничтожение информации - операция уничтожения информации проводится только пользователем с ролью "пользователь, уничтожающий информацию".

Обсуждение

Рассмотрим работу модели в частных случаях.

1. Что запрещает пользователю копировать классифицированную сущность в неклассифицированную?

Классификация данных копируется вместе с данными. В данном случае нарушаются ограничения 2 и 9, если только пользователь не выполняет роль пользователя, уменьшающего классификацию информации. Если данная операция относится к объекту, она попадает под ограничение 3.

2. Что происходит при копировании части объекта в другой объект?

Часть объекта наследует классификацию всего объекта (ограничение 3). Таким образом, перемещение части объекта в другой объект запрещено ограничениями 2 и 3 до тех пор, пока классификация принимающего объекта меньше классификации объекта-источника.

3. Имеет ли пользователь уровень "login"?

Уровень ***login -*** необязательная часть модели, но ее эффект может быть использован посредством классификации терминалов. Классификация терминала - верхняя граница классификации информации, которая может быть просмотрена на нем (ограничение 4). Если пользователь желает ограничить уровень классификации, просматриваемой на терминале, он может вызвать операцию, понижающую классификацию информации, появляющейся на терминале. Корректное определение классификации разделяемых устройств (диски, принтеры и т.д.) устанавливается офицером безопасности. Отметим, что ограничение классификации информации, появляющейся на терминале, не ограничивает классификации информации, с которой может работать субъект.

4. Процесс не присутствует в модели, но присутствует в реализации. Как может быть ограничена его активность?

Операции, также как процессы и программы, присутствуют в модели. Каждая

функция системы должна рассматриваться пользователем как операция. При реализации процессы ограничены операциями, которые соблюдают ограничения безопасности.

5. Какие сущности в системе объекты, а какие контейнеры?

Файл - это контейнер, а группа дата-время - это объект. Если некоторые сущности данного типа - объекты, а некоторые - контейнеры, то должна быть определена функция, позволяющая определить тип сущности, принадлежащей данному семейству.

6. Как создаются сущности?

Для каждого типа сущностей, которые пользователь может создавать, в системе существуют операции, создающие экземпляр данного типа. Как и с другими операциями, это могут делать только пользователи, авторизованные для этого. В частности, только пользователи с авторизованной ролью могут создавать определенные типы сущностей.

7. Как пользователь обращается к объектам или контейнерам?

Некоторые сущности имеют идентификатор, который позволяет адресовать их непосредственно. Сущность может иметь ноль, один или более идентификаторов. Сущность может также быть адресована косвенно с помощью квалифицированного имени.

8. Какая политика управляет доступом к сущности в контейнере?

Ответ на данный вопрос зависит от типа доступа и ссылки (прямая или косвенная). Если сущность адресуется напрямую для просмотра, срабатывает ограничение 4. Если ссылка косвенная, возможны два случая, зависящие от того, находится ли сущность в контейнере, требующем доверия. Если это так, то срабатывают ограничения 4 и 5, иначе срабатывает ограничение 4. Пользователь может просмотреть сущность в контейнере, требующем доверия, если он обратился к ней напрямую, но не может просмотреть ее при косвенном обращении.

9. Имеется ли в системе что-то, что является не пользователем и не сущностью?

С точки зрения пользователя - нет. В реализации могут быть структуры, которым трудно назначить правильную классификацию (например системные очереди). Но все, что пользователь может создать, просмотреть или модифицировать, должно быть пользователем или сущностью.

10. В модели нет уровней целостности. Что предотвращает случайную или умышленную модификацию данных?

Модификация степеней доверия, множества ролей и классификаций определена данными ограничениями безопасности. Для изменения данных пользователь должен запросить операцию; ограничение 1 требует того, чтобы пользователь был авторизован

для данной операции. В принципе, особые случаи можно добавить как специфичные ограничения.

Заключение

Наряду с неоспоримыми достоинствами моделей предоставления прав, выражающимися в их интуитивной понятности и возможности реализации с высокой степенью точности, данные модели имеют ряд недостатков.

В моделях предоставления прав возможно образование скрытых каналов утечки информации. Таким образом, несмотря на кажущуюся простоту реализации систем предоставления прав, перекрытие каналов утечки информации является нетривиальной задачей. При анализе защищенных вычислительных систем, построенных по принципу предоставления прав, необходим тщательный анализ каналов утечки информации. Для систем высокой степени доверия данный пункт отражен в требованиях к системе.

Анализ скрытых каналов утечки информации базируется обычно на принципах анализа потоков данных в программном обеспечении, контроле совместно используемых ресурсов, которые могут быть применены для организации скрытых каналов утечки информации (каналы утечки информации на основе хранения) и использования программами таймеров (временные каналы утечки информации).

Хотя каналы утечки информации нетрудно обнаружить, их обычно находят уже после того, как система синтезирована. Как следствие, их ликвидация может быть затруднительна.

Список цитируемых источников

1.Carl E. Lendwehr, Constanse Leitmeyer, 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 4. Updating of model of mandatory access for military and nuclear systems)

The model of information technologies critical IMS on the basis of granting the rights in the form of mandatory access to objects of complex measurements, modified for military and nuclear appendices is considered.
The basic assumptions and restrictions for the given kind of updatings are presented. Not formalized model of the description of processes of granting of the rights for systems of a similar class is offered.